Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

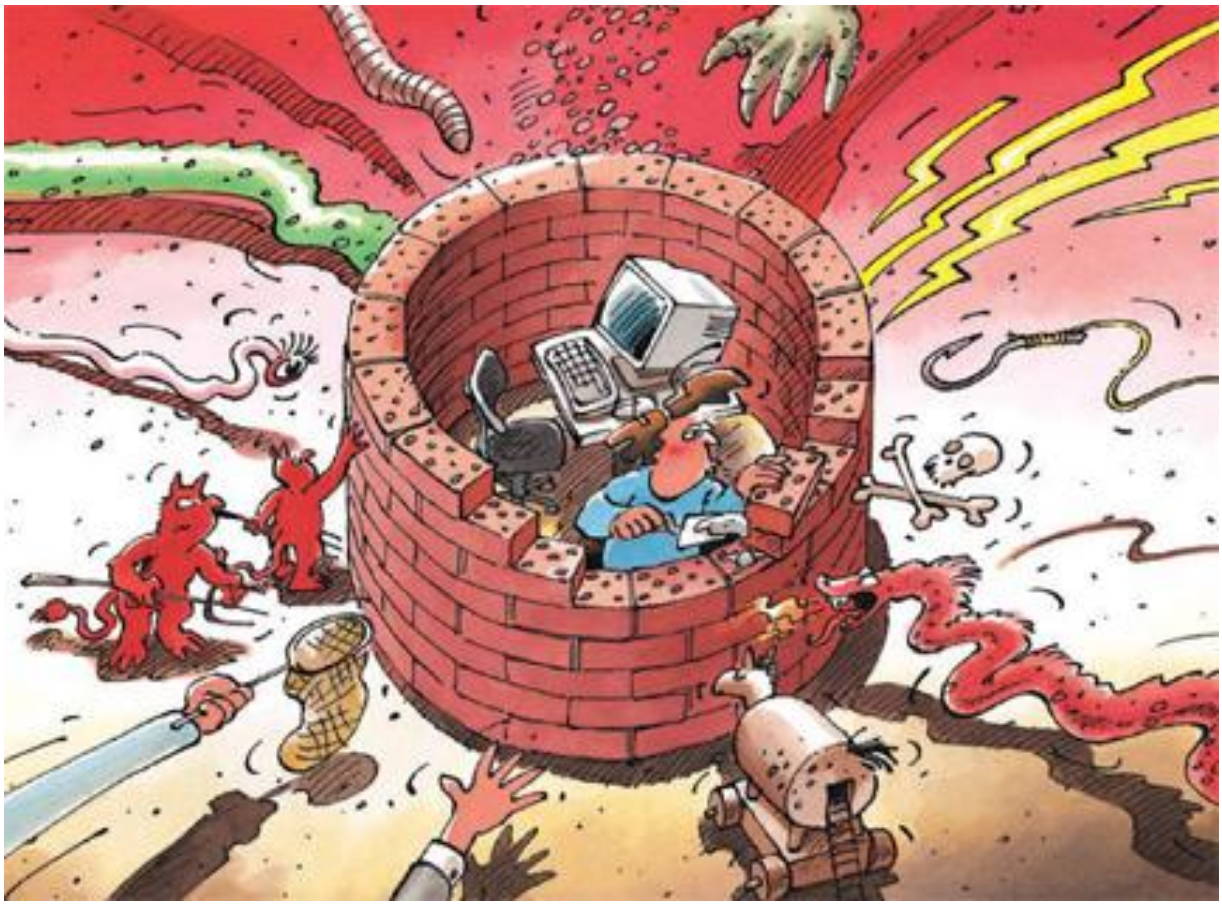
Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI
www.melani.admin.ch

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2013/II (Juli - Dezember)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2013/II 3

2 Einleitung 4

3 Aktuelle Lage IKT-Infrastruktur national 5

3.1 Erpressung durch Cryptolocker & Co 5
3.2 Werbebanner verteilen Schadsoftware 6
3.3 Webseiten mehrfach kompromittiert 7
3.4 Vorschussbetrug – professionalisiert 8
3.5 Bankauszüge an falsche Adressen 9
3.6 Daten beim Schengener Informationssystem gestohlen: auch Schweiz betroffen 10
3.7 NZZ nicht erreichbar - technische Probleme 10
3.8 Die Schweiz gewinnt ersten Cyber Security Alpen Cup 11
3.9 Malware auch auf Linux-Systemen 12
3.10 NTP-Amplifikations-Angriffe - bereits Schweizer Infrastruktur missbraucht 13

4 Aktuelle Lage IKT-Infrastruktur International 14

4.1 Weitere Enthüllungen zu NSA und GCHQ 14
4.2 APT - neue Methoden 17
4.3 Millionen von Adobe-Kundendaten gestohlen 18
4.4 Angriffe bei Target-Verkaufsstellen 19
4.5 SIM-Zweitkarten und ihre Folgen 20
4.6 Gehackter DES-Algorithmus und die Folgen für SIM-Karten 20
4.7 Industrielle und private Kontrollsysteme 21
4.8 Der Syrien-Konflikt – Informationskrieg 2.0 22
4.9 Wenn DDoS von anderen Angriffen ablenkt 23
4.10 Hacker und Schmuggler unter einer Decke 23
4.11 EU-Parlament verabschiedet härtere Strafen für Cyberkriminelle 24

5 Tendenzen / Ausblick 25

5.1 Das Internet am Scheideweg oder Business as usual? 25
5.2 Bitcoin - der Erfolg und sein Preis 26
5.3 Die Rolle von Cyber bei Konflikten 28
5.4 Virendetektion im 21. Jahrhundert - Was kommt nach den signaturbasierten Antivirenprogrammen? 29
5.5 Angriffe auf Heimrouter 33
5.6 Parlamentarische Geschäfte mit Bezug zu Themen im Bereich Informationssicherung 34

6 Glossar 36

1 Schwerpunkte Ausgabe 2013/II

- **Weitere Enthüllungen zu NSA und GCHQ**
  Auch im zweiten Halbjahr 2013 waren die diversen veröffentlichten Aktivitäten basierend auf den Dokumenten von Edward Snowden rund um die US-National Security Agency (NSA) und das Britische General Communication Headquarter (GCHQ) ein grosses Thema. Im zweiten Halbjahr vervollständigte sich das Bild einer flächendeckenden und vollumfassenden Datenerfassung durch diese Nachrichtendienste. Die Erkenntnisse zeigen die Probleme auf, die eine solch transnationale Einrichtung wie das Internet mit sich bringt, an der jedes Individuum, jeder Staat so teilhaben kann und vorgehen darf, wie es ihm gerade beliebt und die nationalen Gesetze es zulassen, ohne dabei auf die globalen Auswirkungen Rücksicht nehmen zu müssen.

  ► Aktuelle Lage International: Kapitel 4.1
  ► Tendenzen / Ausblick: Kapitel 5.1

- **Bitcoin: der Erfolg und sein Preis**
  Bitcoin ist eine dezentrale digitale Währung, das heisst sie hängt von keiner zentralen Ausgabestelle ab. Dadurch unterscheidet sie sich nicht nur von den traditionellen, sondern auch von anderen digitalen Währungen. Mit zunehmender Popularität von Bitcoin stellen sich Fragen insbesondere in Bezug auf das Sicherheitsniveau aber auch den Rechtsstatus und die Regulierung dieser Devisen.

  ► Tendenzen / Ausblick: Kapitel 5.2

- **Ransomware auf dem Vormarsch**
  Bei Ransomware (auf deutsch erpresserische Schadsoftware) sehr verbreitet, sind die Sperrtrojaner, welche auf infizierten Computern eine Meldung anzeigen, die scheinbar von einer Polizeibehörde stammt. Weit schwerwiegender ist eine Infektion mit der Schadsoftware Cryptolocker, welche in der Schweiz das erste Mal im November 2013 beobachtet worden ist. Hier werden alle Daten, die sich auf der Festplatte und auf allen anderen angeschlossenen Datenträgern befinden, verschlüsselt und sind damit für das Opfer nicht mehr zugänglich.

  ► Aktuelle Lage Schweiz: Kapitel 3.1

- **Grosse Datendiebstähle**
  Wieder sind Datendiebstähle bekannt geworden, welche mehrere Millionen Datensätze betroffen haben. Bei Adobe waren nach eigenen Angaben 38 Millionen Kundendaten, Passwörtern und Kreditkartendaten betroffen. Die Ladenkette Target war ebenfalls Opfer eines grossen Datendiebstahls. Laut den publizierten Informationen wurden 40 Millionen Kreditkarten- und 70 Millionen Kundendaten gestohlen.

  ► Aktuelle Lage International: Kapitel 4.3, Kapitel 4.4

- **Industrielle und private Kontrollsysteme – Immer mehr Systeme am Internet**
  Es ist mittlerweile relativ einfach und günstig, Systeme mit Fernabfrage- und -steuerungsfunktion zu beziehen oder eine bestehende Anlage mit einer Kommunikationsschnittstelle nachzurüsten. Entsprechend ist neben Funktion und Benutzerfreundlichkeit einer Fernzugangslösung auch dem Schutz vor unbefugten Manipulationen Beachtung zu schenken. MELANI hat hierzu im Oktober 2013 eine Checkliste zum Schutz von industriellen Kontrollsystemen publiziert.

  ► Aktuelle Lage International: Kapitel 4.7

2 Einleitung

Der achtzehnte Halbjahresbericht (Juli – Dezember 2013) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet Themen im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (*Wörter in kursiv*) sind in einem **Glossar (Kapitel 6)** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

Ausgewählte Themen dieses Halbjahresberichtes sind in **Kapitel 1** angerissen.

Kapitel 3 und 4 befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der zweiten Hälfte des Jahres 2013 aufgezeigt. Kapitel 3 behandelt dabei nationale Themen, Kapitel 4 internationale Themen.

Kapitel 5 enthält Tendenzen und einen Ausblick auf zu erwartende Entwicklungen.

Erstmals enthält **Kapitel 5** ausgewählte parlamentarische Geschäfte mit Bezug zu Themen im Bereich Informationssicherung.

3 Aktuelle Lage IKT-Infrastruktur national

3.1 Erpressung durch Cryptolocker & Co

Ransomware, erpresserische *Schadsoftware*, mit der die Besitzer der infizierten Rechner erpresst werden sollen, gibt es bereits seit geraumer Zeit. Sehr verbreitet sind die sogenannten Sperrtrojaner, welche auf infizierten Computern eine Meldung anzeigen, die scheinbar von einer Polizeibehörde wie dem deutschen Bundeskriminalamt oder dem Eidgenössischen Justiz und Polizeidepartment (EJPD) stammt. Diese verlangt die Zahlung einer Busse unter dem Vorwand, auf dem infizierten Computer illegale Daten gefunden zu haben. Bei Nichtbezahlung bleibe, respektive werde der Computer gesperrt. Diese Art von Schadsoftware ist im Vergleich zu anderer Ransomware aber relativ harmlos, da sie keinen eigentlichen Schaden an Dateien auf dem Computer anrichtet und die Sperre mit relativ einfachen Mitteln aufgehoben werden kann.

Indem der Computer mit einer dem neusten Stand entsprechenden *Antivirus-Live-CD* analysiert wird, kann der Schädling in den meisten Fällen entfernt werden. Eine Anleitung, wie man eine AntiVirus-Live-CD herstellt und benutzt, ist auf den Seiten der Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK zu finden.[1]

Weit schwerwiegender ist aber eine Infektion mit der Schadsoftware Cryptolocker, welche in der Schweiz das erste Mal im November 2013 beobachtet worden ist. Hier werden alle Daten, die sich auf der Festplatte und auf allen anderen angeschlossenen Datenträgern befinden, verschlüsselt und sind damit für das Opfer nicht mehr zugänglich. Es ist zwar davon auszugehen, dass die Verbreitung innerhalb der Schweiz relativ gering ist. Dennoch sind die persönlichen Geschichten, die hinter jedem einzelnen Fall stecken, dramatisch: Privatpersonen verlieren ihre ganze digitale Vergangenheit. Bei KMUs sind oft wichtige Geschäftsdaten betroffen, was bis zur Bedrohung der Existenz führen kann, sofern kein entsprechendes *Backup* erstellt worden ist oder das Backup fehlerhaft gewesen ist.

Cryptolocker scheint sich über infizierte E-Mail Anhänge und über präparierte Webseiten, so genannte Webseiteninfektionen oder *Drive-By Downloads*, zu verbreiten. In einigen Fällen war das betroffenen Gerät bereits mit einer anderen Malware infiziert, welche dann Cryptolocker nachlädt. Es gibt bereits Nachahmer, welche ähnliche Schadsoftware entwickelt haben und in Umlauf bringen.

Nach der Infektion wird dem Opfer eine Meldung präsentiert, in der die Kriminellen eine Geldforderung stellen. Im Gegenzug soll das Opfer den *Schlüssel* erhalten, mit dem die Dateien wiederhergestellt werden können. Verschiedene Antiviren Produkte können zwar die Schadsoftware finden und beseitigen. Meistens ist es jedoch bereits zu spät, weil die auf dem Computer vorhandenen Dateien bereits verschlüsselt worden sind. Das eigentliche Problem ist deshalb nicht die Entfernung der Schadsoftware, sondern die Wiederherstellung der ursprünglichen Daten. Bei bisheriger Ransomware mit integrierter Datenverschlüsselung wurde der Schlüssel fix einprogrammiert und konnte entsprechend einfach aus dem *Quellcode* extrahiert werden. Dies ist mit Cryptolocker nicht mehr möglich: Für jedes Opfer wird auf einem *Command and Control Server* ein eigener Schlüssel generiert. Deshalb scheint es im Moment keine Methode zu geben, die Daten ohne den Schlüssel, der nur den Betrügern

[1] Anleitung zur Herstellung einer Antivirus-Live CD von der Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK: http://www.cybercrime.admin.ch/content/kobik/de/home/dokumentation/informationen/2012-07-06.html

bekannt ist, zu entschlüsseln. Dennoch rät MELANI davon ab, auf die Forderungen der Kriminellen einzugehen und eine Zahlung zu leisten. Denn es gibt keine Garantie, dass die Kriminellen den für das Entschlüsseln der Dateien benötigten Schlüssel dem Opfer auch wirklich zusenden und es ist nicht auszuschliessen, dass die Erpresser die offensichtliche Zahlungsbereitschaft der Opfer ausnutzen und weitere Forderungen stellen.

MELANI hat zusammen mit Schweizer Internet Service Providern (ISP) bereits Massnahmen getroffen, um die Bedrohung durch Cryptolocker zu minimieren.

Cryptolocker zeigt deutlich, wie wichtig es ist, regelmässige Backups durchzuführen und deren Qualität sicherzustellen.

Im Fall von Cryptolocker kommt erschwerend hinzu, dass auch am Computer angeschlossene externe Festplatten von der Verschlüsselung betroffen sind. Besonders tragisch war ein Fall, bei dem Cryptolocker gerade während eines Backupvorgangs zugeschlagen hat und somit Originaldaten und Backupdaten gleichzeitig zerstört hat. Es ist deshalb empfehlenswert, zwei Festplatten jeweils abwechslungsweise zu verwenden und die Backupdatenträger nur während des Backupvorganges anzuschliessen.

Netzlaufwerke sind gemäss aktuellem Stand nicht von der Verschlüsselung betroffen, solange sie keinen *Laufwerksbuchstaben* zugeordnet haben. Jedoch wird die Schadsoftware bestimmt weiterentwickelt, so dass zukünftig möglicherweise auch diese sowie andere Funktionen in der Schadsoftware enthalten sein können.

3.2 Werbebanner verteilen Schadsoftware

AdServer dienen dazu, Werbung auf Websites einzublenden. Die Werbung kann dabei von verschiedenen Werbern und Werbenetzwerken stammen. Bekannte und oft genutzte AdServer sind beispielsweise OpenX und der darauf basierende Revive Adserver. Für Kriminelle sind AdServer ein sehr interessantes Ziel, da so Schadcode in Form manipulierter Werbung via mehrere und zum Teil oft frequentierte Websites sehr einfach verteilt werden kann. Eine gängige Taktik ist dabei das Platzieren eines *Iframes* zusätzlich zum Werbebanner. Ein Iframe ist eine *HTML* Anweisung, welche dazu genutzt werden kann, fremde Inhalte – beispielsweise ein Verweis auf eine Seite mit Schadsoftware – einzubinden.

Erschwerend ist die Tatsache, dass bei OpenX im letzten Halbjahr vermehrt Sicherheitslücken gefunden worden sind. Gepaart mit der Tatsache, dass viele Administratoren die Aktualisierungen nicht zeitnah einspielen, ergibt sich daraus ein erhebliches Sicherheitsrisiko:

So wurde im Juli 2013 in AdServer OpenX eine Sicherheitslücke festgestellt, welche es dem Angreifer ermöglicht, beliebigen *Scriptcode* oder HTML einzuschleusen (*Cross Site Scripting*). Im August 2013 wurde bekannt, dass die freie Version von OpenX über längere Zeit eine *Backdoor* enthielt. Alle Nutzer, die diese Version verwendeten, installierten automatisch auch diese Backdoor, welche Angreifer für ihre Zwecke in die Software eingebaut und auch aktiv ausnutzten. Im September wurde eine weitere Lücke in OpenX und in Revive bekannt, mit welcher registrierte Benutzer beliebigen *PHP Code* auf dem Server ausführen konnten. Im Dezember schliesslich wurde eine sehr gravierende Lücke bekannt, die sowohl OpenX als auch Revive betraf. Diese Lücke bot die Möglichkeit, direkt auf die Datenbank des Servers zuzugreifen (*SQL Injection)*, und die Daten des AdServers zu manipulieren, ohne irgendwelche Zugangsdaten zu besitzen.

In der Schweiz waren verschiedene, teilweise sehr stark genutzte Websites von Vorfällen betroffen. MELANI empfiehlt generell, sämtliche, im Internet exponierte Software

regelmässig zu patchen und in einem *Life Cycle Management* zu halten. Zudem sollten die entsprechenden Logfiles regelmässig überprüft und Anomalien untersucht werden. Die Massnahmen zum Schutz von *Content Management Systemen*[2] können sinngemäss auch auf AdServer angewendet werden. Für OpenX und Revive wird zudem eine Checkliste[3] mit den wichtigsten, regelmässig durchzuführenden Aufgaben angeboten.

3.3 Webseiten mehrfach kompromittiert

Phishingseiten sind ein immerwährendes Problem. Während früher Domänen von den Betrügern extra gelöst worden sind, um die Phishingseite zu platzieren, werden heute vorzugsweise bestehende Internetauftritte auf Schwachstellen überprüft und bei einem Fund ausgenutzt, um eine Phishingseite (meist in einem Unterverzeichnis) zu platzieren. Wie im letzten MELANI Halbjahresbericht 2013/1[4] beschrieben, ist das Finden von Webauftritten mit *Schwachstellen* mit geringem Aufwand verbunden, da viele Webseitenbetreiber ihre *Applikationssoftware* - beispielsweise die Content Management Systeme - nicht regelmässig auf den neuesten Stand bringen.

Ein Ziel von MELANI ist es, dass die Phishingseiten schnellstmöglich aus dem Netz entfernt werden. Zu diesem Zweck schreibt MELANI nach Bekanntwerden einer Phishingseite die Kontaktstelle des Providers (*Abuse-Stelle*) mit der Bitte an, die entsprechende Webseite vom Netz zu nehmen. Hierzu hat es sich international etabliert, dass jeder Webhoster eine Abuse-Stelle betreibt, welche Meldungen über betrügerische Seiten entgegennimmt.

Die Prozesse und Reaktionszeiten, mit welchen betrügerische Seiten entfernt werden, sind allerdings nicht einheitlich geregelt und variieren stark. Während die einen Provider die betroffene Seite sofort selbst vom Netz nehmen, informieren andere Provider zuerst den Webseitenbesitzer und fordern diesen auf, die nötigen Massnahmen zu ergreifen. Erst bei einer Nichtreaktion innerhalb eines vom Provider definierten Zeitraums greift dieser dann selbst ein.

Auch die Verfügbarkeit der Abuse-Stellen ist sehr unterschiedlich. Während einzelne Webhoster einen Rund-um-die Uhr Service anbieten, arbeiten andere nur während Bürozeiten. Dies führt besonders dann zu Verzögerungen, wenn sich der Hoster in einer anderen Zeitzone befindet oder sich der Phishingvorfall am Wochenende oder über die Festtage ereignet.

Doch werden nicht nur Unterschiede bezüglich Schnelligkeit und Verfügbarkeit verzeichnet; auch die Behandlung eines Vorfalles erfolgt nach verschiedenartigen Ansätzen. Wurde beispielsweise eine Schwachstelle in einem CMS ausgenutzt, um eine Phishingseite zu platzieren, reicht es nicht aus, die Phishingseite einfach zu löschen. Zusätzlich muss der Webseitenbesitzer darauf aufmerksam gemacht werden, dass die eingesetzten Applikationen auf den neuesten Stand zu bringen sind. Wird die Aktualisierung unterlassen, führt dies dazu, dass die gleichen Webseiten immer wieder mit erneut platzierten Phishingseiten oder Malware negativ auffallen. Dies zeigt auch folgender Fall deutlich, der im

---

[2] MELANI Checklisten und Anleitungen: Massnahmen zum Schutz von Content Management Systemen (CMS) http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=de (Stand: 20. Februar 2014).

[3] https://checkpanel.com/checklist-templates/openx-maintenance (Stand: 20. Februar 2014). https://checkpanel.com/checklist-templates/revive-maintenance (Stand: 20. Februar 2014).

[4] MELANI Halbjahresbericht 2013/1, Kapitel 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

zweiten Halbjahr 2013 in der Schweiz beobachtet worden ist: Im Zeitraum von Oktober – Dezember 2013 wurde der gleiche Schweizer-Webauftritt insgesamt dreimal hintereinander missbraucht, um Phishingseiten gegen diverse Finanzdienstleister und Kreditkartenfirmen zu platzieren.

Für Hosting-Provider gibt es keine Verpflichtung, einen Abuse-Dienst zu stellen. Ist aber ein Netzwerk nicht ausreichend betreut, gelangt dieses schnell auf eine *Blacklist*. Besonders bei Spam wird dies entsprechend praktiziert. Befindet sich ein Spammer in einem Netzwerk, kann es ohne entsprechende Aktion des Providers schnell passieren, dass der Netzwerkbereich *(IP Range)* in einen Spamfilter gelangt und so sämtliche Kunden keine E-Mails mehr versenden können. Bei Phishingseiten wird dieses Prinzip nicht konsequent angewendet, was den einzelnen Providern einen Spielraum in der Bearbeitung von Phishingseiten lässt.

3.4 Vorschussbetrug – professionalisiert

Neben Kreditkartendaten werden vermehrt auch E-Mail Zugangsdaten gestohlen. Doch wofür werden E-Mail Zugangsdaten eigentlich verwendet? Bekannt aus früheren Halbjahresberichten ist die Betrugsvariante mit E-Mails, die vorgeben, dass der Absender angeblich im Ausland festsitzt und in Schwierigkeiten steckt.[5] Da das E-Mail-Konto in der Hand des Täters ist, kann er dem Opfer vorgaukeln, dass die Kommunikation auch tatsächlich von der dem Opfer bekannten Person stammt. Das Opfer wird dann gedrängt, einen Betrag zu zahlen.

Eine weitere Variante, die immer wieder beobachtet wird, ist das Durchsuchen der E-Mails nach irgendwelcher Kommunikation mit einem Finanzinstitut. Hier wird anschliessend durch die Betrüger versucht, diese Kommunikation mit dem Bankangestellten wieder aufzunehmen und diesen zu überzeugen, eine Zahlung auszulösen. Diese Variante wird vor allem im Ausland beobachtet, es gibt aber auch einzelne Fälle in der Schweiz.

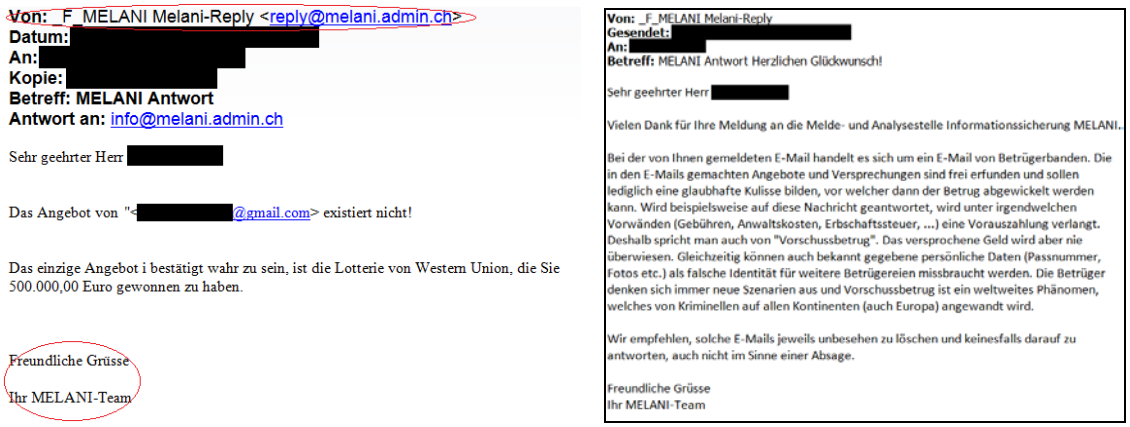
Eine weit perfidere Variante wurde von MELANI Ende 2013 beobachtet. Angefangen hat alles mit einer simplen Vorschussbetrugsmail. In einem solchen Betrugsmail werden dem Opfer jeweils Gewinne oder grosse Geldsummen aus Erbschaften in Aussicht gestellt. Hat das Opfer erst einmal angebissen, folgen dann angebliche, notwendige Vorauszahlungen wie Gewinn-, Erbschaft-, Transaktionssteuern oder anderes. Vom versprochenen Geld sieht das Opfer allerdings nie etwas.

Im beschriebenen Fall war das Opfer skeptisch und entschied sich dann, die Melde- und Analysestelle Informationssicherung (MELANI) anzufragen, ob diese E-Mail echt sei und ob es auf das Angebot eingehen soll. MELANI antwortete wie immer in solchen Fällen mit einer Standardantwort, die Finger von solchen E-Mails zu lassen, diese zu löschen und schon gar nicht mit den Betrügern Kontakt aufzunehmen. Umso erstaunlicher war anschliessend die Reaktion des Opfers, welches nun noch einmal schriftlich nachfragte, ob MELANI wirklich der Ansicht sei, dass das Geschäft in Ordnung sei und ob es wirklich die geforderten Steuern im Voraus bezahlen soll.

Irritiert setzte sich MELANI nun telefonisch mit dem Melder in Kontakt, um klarzustellen, dass diese E-Mail ein Betrugsmail ist und auf keinen Fall eine Einzahlung getätigt werden soll. Beim Telefongespräch wurde sofort klar, dass die Betrüger die E-Mail von MELANI in der

[5] MELANI Halbjahresbericht 2012/1, Kapitel 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 20. Februar 2014).

Inbox des Opfers manipuliert und dahingehend abgeändert hatten, dass das Opfer zur Zahlung ermuntert wurde. Die Betrüger hatten also Zugriff auf das E-Mail Konto des Opfers, um die entsprechende Manipulation vorzunehmen.



Von: _F_MELANI Melani-Reply <reply@melani.admin.ch>
Datum: [redacted]
An: [redacted]
Kopie: [redacted]
Betreff: MELANI Antwort
Antwort an: info@melani.admin.ch

Sehr geehrter Herr [redacted]

Das Angebot von "<[redacted]@gmail.com> existiert nicht!

Das einzige Angebot i bestätigt wahr zu sein, ist die Lotterie von Western Union, die Sie 500.000,00 Euro gewonnen zu haben.

Freundliche Grüsse

Ihr MELANI-Team

Von: _F_MELANI Melani-Reply
Gesendet: [redacted]
An: [redacted]
Betreff: MELANI Antwort Herzlichen Glückwunsch!

Sehr geehrter Herr [redacted]

Vielen Dank für Ihre Meldung an die Melde- und Analysestelle Informationssicherung MELANI.

Bei der von Ihnen gemeldeten E-Mail handelt es sich um ein E-Mail von Betrügerbanden. Die in den E-Mails gemachten Angebote und Versprechungen sind frei erfunden und sollen lediglich eine glaubhafte Kulisse bilden, vor welcher dann der Betrug abgewickelt werden kann. Wird beispielsweise auf diese Nachricht geantwortet, wird unter irgendwelchen Vorwänden (Gebühren, Anwaltskosten, Erbschaftssteuer, ...) eine Vorauszahlung verlangt. Deshalb spricht man auch von "Vorschussbetrug". Das versprochene Geld wird aber nie überwiesen. Gleichzeitig können auch bekannt gegebene persönliche Daten (Passnummer, Fotos etc.) als falsche Identität für weitere Betrügereien missbraucht werden. Die Betrüger denken sich immer neue Szenarien aus und Vorschussbetrug ist ein weltweites Phänomen, welches von Kriminellen auf allen Kontinenten (auch Europa) angewandt wird.

Wir empfehlen, solche E-Mails jeweils unbesehen zu löschen und keinesfalls darauf zu antworten, auch nicht im Sinne einer Absage.

Freundliche Grüsse
Ihr MELANI-Team

Abbildung 1: Links: Gefälschtes E-Mail von den Betrügern, Rechts: Originalmail von MELANI

3.5 Bankauszüge an falsche Adressen

Aufgrund eines Programmfehlers kam es beim Jahresendversand der Bank Coop zum Teil zu Fehlzustellungen: Gewisse Kontoauszüge wurden dadurch an falsche Adressaten gesandt. Die Bank Coop hat die Ursache in der Zwischenzeit eruiert und die Ursache für die falschen Zustellungen gefunden, welche im Zusammenhang mit der Einführung einer neuen Punkteübersicht für das Supercard-Programm steht, an welchem die Bank teilnimmt. Die Empfänger der fälschlicherweise zugestellten Unterlagen sind gebeten worden, diese an die Bank zu retournieren. Die Bank Coop hat versprochen, alle notwendigen Massnahmen zu treffen, damit ein solcher Fehler in Zukunft vermieden werden kann.

In Basel-Stadt, dem Hauptsitz der Bank, hat die Staatsanwaltschaft bekannt gegeben, dass sie ein polizeiliches Ermittlungsverfahren wegen Verdachts der fahrlässigen Verletzung des Bankgeheimnisses eröffnet.

Dieser Vorfall ist kein Einzelfall. So wurde im Februar 2014 bekannt, dass die Wirtschaftsprüferin PricewaterhouseCoopers (PWC) bei einem ähnlichen Zwischenfall einige Lohnausweise an die falschen Mitarbeiter gesendet hat.[6] In der IKT besteht ein klarer Trend, stetig komplexere Programme mit immer mehr Funktionen einzusetzen. Dass bei dieser steigenden Zahl an Programmierzeilen auch das Fehlerrisiko zunimmt, liegt auf der Hand. Ein besonderes Problem liegt bei denjenigen Applikationen, welche nur im laufenden Betrieb geändert respektive aktualisiert werden können. Obschon hier jeweils zahlreiche Versuche im Vorfeld auf Testsystemen durchgeführt werden, können nicht alle Abhängigkeiten, welche in solchen Programmen zuhauf vorhanden sind, getestet werden.

[6] http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/PWCMitarbeiter-erhalten-Lohnausweise-der-Kollegen/story/26934239 (Stand: 20. Februar 2014).

3.6 Daten beim Schengener Informationssystem gestohlen: auch Schweiz betroffen

Im Dezember berichteten verschiedene Schweizer Medien über einen Datendiebstahl beim Schengener Informationssystem (SIS). Das SIS erfasst gestohlene Gegenstände und polizeilich gesuchte Personen, für die ein Auslieferungsantrag, ein Einreiseverbot oder eine Vermisstenmeldung vorliegt. Zugriff auf die Datenbank haben die Polizei- und Zollbehörden im Schengenraum.

Der Angriff erfolgte über eine Sicherheitslücke bei der Firma, die 2012 die Datenbank für die dänische Polizei verwaltete. Bei einem grenzüberschreitenden System wie dem SIS sind bei einer Lücke potenziell die Daten aller angeschlossenen Länder betroffen. Die Schweiz wurde im Mai 2013 informiert. Von den 1,2 Millionen gestohlenen Daten stammten 26'478 Einträge von Schweizer Behörden. Der gestohlene Ordner enthielt Personen- und kodierte Daten, der den Grund des Eintrags enthielt. Diese sind nicht direkt lesbar und grundsätzlich konnten so keine Personen dem Eintragsgrund in der Liste zugeordnet werden. Die Lücke betrifft nur das System SIS 1, das im Mai 2013 durch SIS 2 abgelöst wurde.

Die Einzelheiten des Angriffs (Methode, Lücke) und die Motive der Angreifer sind weiterhin unklar. Diese dürften wohl erst nach Abschluss der Untersuchungen in Dänemark publiziert werden. Laut den dänischen Behörden wurde die Lücke aber geschlossen. Die deutschen Behörden haben zudem bei einer Anfrage eines Abgeordneten zu einzelnen Punkten Stellung genommen. Sie gehen von einem ungezielten, nicht gegen das SIS gerichteten Angriff aus. Es wurde eine Lücke auf einem Server genutzt, der auch andere Daten enthielt. Zwei Hacker, ein Däne und ein Schwede, sollen die Hand im Spiel gehabt haben.

Dieser Vorfall zeigt eine wesentliche Problematik bei der Spezifikation und Implementierung von Systemen zum internationalen Austausch von heiklen und sensitiven Daten auf. Oftmals werden solche Systeme auf politischer Ebene in erster Linie darauf spezifiziert, welche Art der Daten ausgetauscht werden sollen. Technische Anforderungen zur Implementierung werden entweder nur untergeordnet behandelt, oder aber den einzelnen Mitgliedsstaaten überlassen. Damit einher geht das Risiko, dass bei einer suboptimalen Umsetzung in einem Mitgliedsstaat die Daten anderer Länder ebenfalls in Mitleidenschaft gezogen werden. Entsprechend ist in Zukunft auch bei anderen Projekten zum Informationsaustausch immer darauf zu bestehen, dass nicht nur die Definition der auszutauschenden Daten vorliegt, sondern auch ein für alle gültiger Mindeststandard bei der Sicherung, Bearbeitung und technischen Übermittlung klar vordefiniert wird.

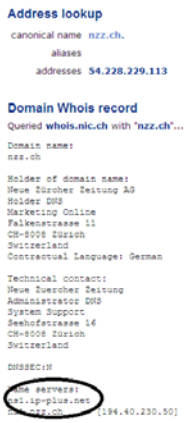
3.7 NZZ nicht erreichbar - technische Probleme

Am 19. August 2013 war die Webseite der NZZ für einige Besucher nicht mehr erreichbar. Zuerst wurde eine Attacke hinter diesem Vorfall vermutet. Grund dieses teilweisen Ausfalles war aber laut Swisscom ein Fehler bei der Verlängerung der Domainregistrierung zwischen der Registrierungsstelle Networksolutions und der Swisscom.

Die Domäne ip-plus.net der Swisscom war zu diesem Zeitpunkt bei der Firma Networksolutions registriert. Diese hatte am 19. August 2013 um 12:40 Uhr die *Domäne* gekappt, so dass ip-plus.net nicht mehr aufgelöst werden konnte und damit nicht mehr funktionierte. Da unter dieser Domäne auch *DNS-Dienste* von Drittfirmen wie zum Beispiel der NZZ liefen, waren zwangsläufig auch diese Seiten ausgefallen und nicht mehr erreichbar. Das Problem konnte zwar bereits um 15:25 Uhr von der Swisscom behoben werden und auch die IT-Abteilung der NZZ hatte sofort alle betroffenen Server aus den DNS-Einträgen gelöscht und durch funktionierende Server ersetzt. Da die jeweiligen

Fehlauflösungen jeweils 24 Stunden im Name Server und *Internet Explorer Cache* gespeichert bleiben, dauerte es aber bis zu 24 Stunden, bis alle Dienste wieder einwandfrei funktionierten.[7]

Swisscom hat nach diesem Vorfall per sofort Massnahmen umgesetzt, die einen weiteren vergleichbaren Ausfall ausschliessen werden.


Address lookup
canonical name nzz.ch.
aliases
addresses 54.228.229.113

Domain Whois record
Queried whois.nic.ch with "nzz.ch"...
Domain name:
nzz.ch

Holder of domain name:
Neue Zürcher Zeitung AG
Holder DNS
Marketing Online
Falkenstrasse 11
CH-8008 Zürich
Switzerland
Contractual Language: German

Technical contact:
Neue Zuercher Zeitung
Administrator DNS
System Support
Seehofstrasse 16
CH-8008 Zürich
Switzerland

DNSSEC:N

Name servers:
ns1.ip-plus.net
[194.40.230.50]

Abbildung 2: Whois Eintrag der NZZ mit dem DNS Server von ip-plus.net

Mit Hilfe des Domain Name Systems (DNS) lassen sich das Internet und dessen Dienste benutzerfreundlich verwenden, da man anstelle von IP-Adressen Webadressen (URL) verwenden kann. Ohne DNS-Server ist das Internet immer noch funktionsfähig, es müssen aber an Stelle der URL die IP-Nummern eingegeben werden. Bei diesen befinden sich zuoberst in der Hierarchie die Root-Server, welche als oberste Instanz für Informationen betreffend Top-Level-Domains (z. B. .com, .net, .ch) zuständig sind. Die unteren Instanzen (Second Level Domains) werden durch zahlreiche grosse und kleine Internet-Dienstleister betrieben. Eine Störung oder eine Manipulation kann jeweils weitreichende Folgen haben, insbesondere wenn es sich wie in diesem Fall um einen wichtigen DNS-Server eines grossen Unternehmens handelt.

3.8 Die Schweiz gewinnt ersten Cyber Security Alpen Cup

Um dem Problem von fehlenden Cyber Security Spezialisten im Land vorzubeugen und gleichzeitig der Wirtschaft die Suche nach Talenten zu erleichtern, initiierte der Verein Cyber Security Austria (CSA) im Jahr 2012 den Cyber Security Challenge. In diesem in Kooperation mit dem Kuratorium Sicheres Österreich (KSÖ) und dem Abwehramt durchgeführten Wettbewerb kämpften hunderte von Schülern in einem via Internet durchgeführten Auswahlverfahren um den Sieg.

Im Jahr 2013 übernahm der Verein Swiss Cyber Storm unter dem Patronat der Melde- und Analysestelle Informationssicherung (MELANI) des Bundes und dem Verein Swiss Police ICT diese Idee.[8] Unter der Federführung von Cyber Security Austria wurde daraufhin die Durchführung eines länderübergreifenden Wettkampfs sowie eine Erweiterung des Teilnehmerfeldes auf Schüler und Studenten beschlossen. Der Security Alpen Cup war geboren.

---

[7] http://www.nzz.ch/aktuell/digital/nzz-dns-1.18135806 (Stand: 20. Februar 2014).

[8] MELANI Halbjahresbericht 2013/1, Kapitel 3.9: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

Vom 5. bis 7. November 2013 fand in Linz somit der erste Cyber Security Alpen Cup statt. Nach einem Tag mit Teambuilding-Aktivitäten und Zeit zum Kennenlernen, fand am zweiten Tag der eigentliche Teamwettkampf statt. Mehr als elf Stunden lang versuchten die beiden Teams aus Österreich und der Schweiz Codes zu entschlüsseln, Sicherheitslücken zu finden und mögliche Zugänge zu Mobiltelefonen und Tablets zu finden. Es ging dabei nicht nur um den Angriff, sondern auch um Massnahmen, um unbefugte Zugriffe zu verhindern. Das Team Schweiz ging schliesslich als Sieger aus dem Wettbewerb hervor und durfte bei der Preisverleihung im Heeresgeschichtlichen Museum in Wien, bei der zahlreiche Gäste aus Politik, Militär und Wirtschaft anwesend waren, den Siegerpokal entgegen nehmen.

Das Konzept eines Cyber Security Wettbewerbs als Plattform zur Talentsuche und Nachwuchsförderung sowie dessen erfolgreiche Umsetzung im ersten Security Alpen Cups ist nicht unbemerkt geblieben: Nächstes Jahr wird sich auch Deutschland am Wettbewerb beteiligen. Die Schweizer Ausscheidung für den Länderkampf wird wiederum im Rahmen der IT Security Konferenz Swiss Cyber Storm stattfinden, deren 5. Ausgabe am 22. Oktober 2014 im KKL Luzern stattfindet. Interessierte Schüler und Studenten können sich auf www.verbotengut.ch bereits vorregistrieren.

3.9 Malware auch auf Linux-Systemen

Nicht nur Windows (Microsoft) und OSX (Apple) Systeme sind von Schadsoftware betroffen, sondern auch Unix / Linux. In der zweiten Jahreshälfte 2013 wurden MELANI diverse kompromittierte Unix / Linux Systeme in der Schweiz gemeldet, welche mit einem ausgeklügelten *Rootkit* Namens Ebury infiziert wurden. Dabei gelang es Kriminellen, auf bisher unbekannte Weise, Zugriff auf das System des Opfers zu erhalten und das Ebury *Rootkit* zu installieren. Dabei wird üblicherweise der auf dem System des Opfers installierte *SSH-Daemon* so modifiziert, dass die Zugangsdaten sämtlicher Benutzer, welche sich nach dem Zeitpunkt der Infektion an dem infizierten System via SSH anmelden, an die Kriminellen abfliessen. Zusätzlich stiehlt das Ebury Rootkit auf dem System vorhandene private SSH-Schlüssel. Mit den gestohlenen Zugangsdaten können sich die Angreifer jederzeit Zugang zum infizierten System verschaffen und dieses für illegale Zwecke, wie z. B. *Hosting* von *C&C Servern* oder Versand von *Spam* Emails verwenden.

Da es sich bei Ebury um eine Schadsoftware mit Rootkit-Funktionalität handelt, ist diese auf infizierten Systemen schwer zu erkennen. Zudem verwendet Ebury als Kommunikations-Kanal zwischen einem mit Ebury infizierten System und den Kriminellen ein DNS-basiertes Protokoll. Dies erschwert in vielen Fällen das Erkennen der Infektion zusätzlich.

Weitere Informationen zu Ebury und wie diese Schadsoftware detektiert werden kann, finden sich auf der Webseite des deutschen CERT-Bund.[9]

Open Source wird oftmals zu Recht als mögliche Alternative für den Einsatz so genannter proprietärer Softwarelösungen postuliert. Allerdings greift dabei die Logik, dass *Open Source* nachvollziehbar und damit eben sicherer ist, zu kurz. Zwar erlauben Open Source Lösungen jedem, den Programmcode nach Fehlern zu untersuchen. Sollte ein solcher aber nie gefunden und somit von der Community nicht behoben werden, wird auch bei Open Source Lösungen ein Angriffsvektor verbleiben. Insofern ist beim professionellen Einsatz von Open Source Lösungen zu bedenken, dass ein In-Haus-Team die eingesetzte Software nach den Prioritäten des Betriebes untersucht, um nicht abhängig von den Interessen der Open

[9] https://www.cert-bund.de/ebury-faq (Stand: 20. Februar 2014).

Source Community zu sein. Diese Tatsache ist bei der wirtschaftlichen Abwägung des Einsatzes zwischen Open Source oder *proprietären Systemen* entsprechend einzubeziehen.

3.10 NTP-Amplifikations-Angriffe - bereits Schweizer Infrastruktur missbraucht

Auch in den vergangenen Monaten waren die so genannten *Distributed Denial Of Service* (DDoS)-Attacken eine von Cyberkriminellen häufig verwendete Methode, um die Erreichbarkeit bestimmter Dienste oder Websites einzuschränken oder sogar auszusetzen. Dabei lassen sich verschiedene Angriffsarten unterscheiden: Nachdem im letzten Halbjahr die DNS-Amplifikation-Angriffe[10] stark zugenommen haben, welche Angriffe um den Faktor 20 bis 50 verstärken (siehe hierzu den MELANI-Halbjahresbericht 2013/1[11]), ist im zweiten Halbjahr 2013 in ähnlicher Art und Weise nun auch das *NTP-Protokoll*, das dem Zeitabgleich im Internet dient, für DDoS Angriffe missbraucht worden. Dabei fordern die Angreifer mit gefälschter Absenderadresse bei NTP-Servern Daten an. Die um ein Vielfaches grössere Antwort geht dann an die vermeintliche Absenderadresse, also an das tatsächliche Angriffsziel. Weil die Antworten legitime Daten sind, die von zulässigen Servern kommen, ist es besonders schwierig, diese Art von Angriffen abzublocken. NTP-Angriffe sind noch weit wirksamer als DNS-Amplifikations-Angriffe und können eine Verstärkung um den Faktor 500 auslösen.[12] MELANI wurde bereits auf mehrere NTP Server in der Schweiz aufmerksam, die für Angriffe missbraucht wurden.

NTP-Angriffe basieren auf der Ausnutzung des Befehles «monlist» – ein Feature, das in älteren NTP fähigen Geräten standardmässig eingeschaltet ist.[13] Dieser Befehl gibt eine Liste mit den 600 *IP-Adressen* heraus, welche sich zuletzt auf den NTP-Server verbunden haben. Wird die Ursprungsadresse gefälscht, wird so die gesamte Liste an das Opfer gesendet.

Um zu verhindern, dass ein NTP-Gerät für solche Angriffe missbraucht wird, kann die Funktion «monlist» deaktiviert oder auf die neueste NTP-Version aktualisiert werden, welche diese Funktionalität standardmässig deaktiviert.

In Anbetracht der Zunahme von DDoS-Angriffen ist es für jedes Unternehmen empfehlenswert, dessen Geschäftstätigkeit von der Erreichbarkeit ihrer Webseite und/oder der Internetkonnektivität abhängig ist, die Risiken solcher Angriffe abzuklären und Abwehrmassnahmen zu planen. Dies beinhaltet neben eigenen technische Massnahmen zur Erkennung und Abwehr typischerweise auch die Einschätzung der Fähigkeiten des Upstream-Providers und dessen vertragliche Verpflichtungen im Ereignisfall.

---

[10] Bei einer DNS Amplifikationsattacke werden gefälschte DNS-Anfragen an offene DNS-Server im Internet gesendet. Da die Quell-IP Adressen gefälscht sind, werden die Antworten an die IP-Adresse des Opfers und nicht an den tatsächlichen Absender des Datenpakets gesendet.

[11] MELANI Halbjahresbericht 2013/1, Kapitel 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

[12] http://www.zdnet.de/88184056/rekord-ddos-angriff-europa-erreicht-400-gbits/?ModPagespeed=noscript (Stand: 20. Februar 2014).

[13] https://www.us-cert.gov/ncas/alerts/TA14-013A (Stand: 20. Februar 2014).

4 Aktuelle Lage IKT-Infrastruktur International

4.1 Weitere Enthüllungen zu NSA und GCHQ

Auch im zweiten Halbjahr 2013 waren die von diversen Journalisten basierend auf den Dokumenten von Edward Snowden veröffentlichten Aktivitäten rund um die US-National Security Agency (NSA), das Britische General Communication Headquarter (GCHQ) und weitere ausländische Nachrichtendienste ein grosses Thema. Nach den ersten Enthüllungen zu Prism, XKeyscore und Tempora, welche MELANI bereits im letzten Halbjahresbericht[14] thematisiert hatte, vervollständigte sich im zweiten Halbjahr stetig das Bild einer flächendeckenden und vollumfassenden Datenerfassung durch US- und Britische Nachrichtendienste. So wurde beispielsweise bekannt, dass die NSA, analog zur Britischen Operation Tempora, ein Programm mit dem Namen Upstream unterhält[15], um an Glasfaserdaten zu gelangen. Diese Zusammenarbeit mit US-Telekommunikationsfirmen soll die NSA im Jahr 2013 rund 278 Millionen Dollar gekostet haben.[16] Im Weiteren wurde ein gemeinsames Projekt von NSA und GCHQ mit dem Codenamen Muscular bekannt, das zum Ziel hat, sich Zugriff zu den Verbindungen der Rechenzentren von Google und Yahoo zu verschaffen.[17] Das veröffentlichte Dokument beziffert die abgefangenen Datensätze auf 181 Millionen innerhalb von 30 Tagen. Einen anderen Einblick in die Grössenordnung gibt ebenfalls eine von 2012 datierte Präsentation, welche zeigt, dass die NSA weltweit 50‘000 Computernetzwerke mit Malware infiziert haben soll, um an sensible Daten zu kommen.[18] Ein im Januar 2014 veröffentlichtes Dokument spricht von 100‘000 von der NSA gehackten Computern.[19]

Es war aber nicht nur die Dimension, die für Debatten sorgte – auch die Ziele, welche die NSA im Visier hatte, sorgten für Diskussionsstoff. So wurde das primäre Ziel der Aufklärung stets in der Terrorismusabwehr gesehen. Der Umstand, dass bei diversen Abhöraktionen auch Regierungschefs und Diplomaten im Visier stehen, machte allerdings schnell klar, dass auch eine politische Komponente mitschwingt. In Lateinamerika sorgte das Abhören der brasilianischen Präsidentin Rousseff, des jetzigen mexikanischen Präsidenten Peña Nieto und des früheren Mexikanischen Präsidenten Felipe Calderón für Entrüstung.[20] Auf internationaler Ebene war die angebliche Abhöraktion am G8/G20 Gipfel in Toronto[21] ein

---

14 MELANI Halbjahresbericht 2013/1, Kapitel 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

15 http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (Stand: 20. Februar 2014).

16 http://www.heise.de/newsticker/meldung/Ueberwachungsaffaere-NSA-zahlt-Hunderte-Millionen-Dollar-an-Provider-1945984.html (Stand: 20. Februar 2014).

17 http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (Stand: 20. Februar 2014).

18 http://www.spiegel.de/netzwelt/netzpolitik/nsa-soll-50-000-netzwerke-weltweit-infiltriert-haben-a-935335.html (Stand: 20. Februar 2014).

19 http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0 (Stand: 20. Februar 2014).

20 http://www.bbc.co.uk/news/world-latin-america-23938909 (Stand: 20. Februar 2014).

21 http://www.spiegel.de/netzwelt/netzpolitik/kanada-erlaubte-nsa-spionage-bei-g-8-gipfel-a-936255.html (Stand: 20. Februar 2014).

Thema und in Europa dürfte die Abhöraktion gegen das Mobiltelefon der deutschen Bundeskanzlerin Angela Merkel am meisten Schlagzeilen gemacht haben.[22]

Ebenfalls publik wurde die Operation Socialist[23]. Diese bestand aus einem Angriff auf die Belgacom Tochter Bics (ein Joint-Venture der Belgacom mit der Swisscom und der südafrikanischen MTM). Grosskunden dieses Telekommunikationsunternehmens sind unter anderem die EU-Kommission, der Rat der Mitgliedstaaten und das Europaparlament.

Operation Socialist / Angriff auf die Bics

Belgacom hatte im Zuge der NSA-Enthüllungen eine interne Untersuchung veranlasst und einen Angriff festgestellt, der zunächst der NSA zugeordnet wurde. Nach einer weiteren Enthüllung fiel der Verdacht auf das GCHQ, wobei die Briten Technologien eingesetzt haben sollen, die von der NSA entwickelt worden sind. Beim Projekt mit dem Namen «Operation Socialist» soll es um eine «bessere Ausspähung von Belgacom» und um ein «besseres Verständnis der Infrastruktur» gegangen sein. Der Präsentation zufolge wurden dazu gezielt die Computer von Belgacom-Mitarbeitern infiziert und anschliessend versucht, von diesen Computern aus Zugang zu den zentralen *Roaming* Routern zu erlangen.

Dieser Fall betrifft direkt und indirekt auch die Schweiz, da die Swisscom mit 24 Prozent an der BICS beteiligt ist. Die Swisscom selber wiederum gehört zu 51 Prozent dem Schweizer Staat und somit dem Schweizer Steuerzahler.

Korrumpierte Verschlüsselungsstandard?

Aus Sicht der Informationssicherheit ist eine der wichtigsten Fragen, inwieweit Verschlüsselungsprogramme und Verschlüsselungsstandards heute noch vertrauenswürdig sind. Schlagzeilen machte hier vor allem der Standard Dual_EC_DRBG, ein von der NSA entwickelter Zufallszahlengenerator, der die Zahlen nicht so zufällig liefert, wie er es eigentlich sollte: Im Dezember 2013 wurde bekannt, dass die NSA angeblich zehn Millionen US-Dollar an die Firma RSA-Security bezahlt hatte, damit das Security-Unternehmen den umstrittenen Zufallsgenerator in die weitverbreitete Software BSAFE standardmässig implementiert.[24] RSA hat diese Berichte dementiert, die NSA hat auf die Publikation nicht reagiert.

Die Grenzen der Verschlüsselung - Bullrun und Edgehill

Die veröffentlichten Daten zeigen, wie systematisch die beiden Geheimdienste GCHQ und NSA das Thema Entschlüsselung angehen.[25] [26] Die beiden Geheimdienste haben in den letzten Jahren anscheinend eine Menge an Massnahmen und Techniken aufgebaut, um Verschlüsselungen zu brechen oder zu umgehen. Ein Aspekt ist die oben erwähnte Schwächung der Zufallsgeneratoren. Mit solch manipulierten Generatoren sieht die Verschlüsselung zwar stark aus, kann aber mit relativ geringem rechnerischen Aufwand geknackt werden. Auch das «Besorgen» von Schlüsseln ist eine Möglichkeit, mit denen sich verschlüsselte Daten in Echtzeit oder auch nachträglich entschlüsseln lassen.

---

22 http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html (Stand: 20. Februar 2014).

23 http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html (Stand: 20. Februar 2014).

24 http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 (Stand: 20. Februar 2014).

25 http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Stand: 20. Februar 2014).

26 https://www.schneier.com/blog/archives/2013/10/defending_again_1.html (Stand: 20. Februar 2014).

Im Dezember 2013 wurde schliesslich publik, dass die NSA den weltweit am meisten verwendete *Stream* Cipher A5/1, der die Verschlüsselung zwischen Mobiltelefon und Sendemast sicherstellt, einfach knacken kann.[27] So können Anrufe und Text-Meldungen entschlüsselt werden.

Um die gewünschten Daten abzufangen und zu entschlüsseln, bleibt immer noch die Möglichkeit, in die Systeme einzubrechen und die Daten noch vor der Verschlüsselung abzugreifen. Bei der NSA ist hier die sogenannte Abteilung «Tailored Access Operation» (TAO) zuständig.[28]

Weitere Themen, die im Zusammenhang mit der Affäre Snowden im Fokus standen:

Royal Concierge

Die deutsche Wochenzeitschrift Spiegel publizierte im November 2013 einen Artikel über das Überwachungsprogramm Royal Concierge, das vom britischen GCHQ betrieben wird. Es kann die Reservationen in mindestens 350 Luxushotels weltweit überwachen und somit den Aufenthalt von Diplomaten oder hohen Funktionären feststellen.[29]

TOR – direkt nicht knackbar

Der *Anonymisierungsdienst* TOR steht gemäss einer ebenfalls veröffentlichten Präsentation durch Snowden auch in der Aufmerksamkeit der NSA. Zwar konnte die NSA das TOR-Netzwerk nicht direkt knacken, um die einzelnen Nutzer zu enttarnen. Trotzdem scheint es möglich zu sein, einzelne TOR-User anzugreifen, indem Schwachstellen in den Firefox Browsern ausgenutzt werden. Dies sei aber nur durch eine manuelle Analyse bei einem kleinen Teil der TOR-Benutzer möglich, wie auf der Präsentation ersichtlich ist.[30]

Follow the Money - SWIFT

In der Schweiz hat vor allem die Meldung für Aufsehen gesorgt, dass der Finanzdienstleister SWIFT von der NSA ausspioniert werden soll. Eines der drei Rechenzentren von SWIFT befindet sich im thurgauischen Diessenhofen. Hier werden täglich bis zu 15 Millionen Finanztransaktionen abgewickelt. Im Zusammenhang mit dieser Veröffentlichung wurde ebenfalls behauptet, dass es bei der NSA eine Abteilung namens «Follow the Money» gebe, die für das Ausspionieren von Finanzdaten zuständig sei. SWIFT hat erklärt, dass es keinen Grund zur Annahme gebe, dass es jemals zu einem unbefugten Eindringen in ihr Netzwerk gekommen ist.[31]

Die «Signals Intelligence Strategy (SIGINT)» der NSA vom Februar 2012, welche im November 2013 von der New York Times publiziert worden ist, bringt die Strategie der NSA sehr deutlich auf den Punkt:
«Ensure Signals Intelligence provides the decisive edge in advancing the full spectrum of U.S. national security interests.» In order to fulfil this vision, it is ready to «Defeat adversary

[27] http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html (Stand: 20. Februar 2014).

[28] http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html (Stand: 20. Februar 2014).

[29] http://www.spiegel.de/netzwelt/netzpolitik/royal-concierge-britischer-geheimdienst-ueberwacht-diplomatenhotels-a-933997.html (Stand: 20. Februar 2014).

[30] http://www.zdnet.de/88171545/nsa-arbeitet-sich-an-anonymisierungsdienst-tor-ab/?ModPagespeed=noscript (Stand: 20. Februar 2014).

[31] http://www.nzz.ch/aktuell/schweiz/swift-bestreitet-nsa-spionage-1.18151215 (Stand: 20. Februar 2014).

cybersecurity practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere».[32]

Daten sollen also zu jeder Zeit, an jedem Ort und von jeder Person durch die NSA erhalten werden können. Die nun veröffentlichten Publikationen und Daten geben einen Hinweis darauf, dass die Aussage in dieser Strategie nicht nur ein Lippenbekenntnis ist, sondern dass die NSA und ihre Partner diese Strategie auch tatsächlich umsetzen. Die Auswirkungen, die diese Enthüllungen auf die Entwicklung des Internets haben werden, sind momentan noch schwer abzuschätzen.[33] Bereits sind Stimmen laut geworden, welche das Ende des jetzigen Internets voraussagen. Geschäftliche wie auch private Internetnutzer werden sich in Zukunft mit den Auswirkungen der durch Snowden veröffentlichten Informationen in Bezug auf die Risikoeinschätzung vermehrt auseinandersetzen müssen.

4.2 APT - neue Methoden

«NetTraveler» ist ein *APT («Advanced Persistent Threat»)*, der Kaspersky im Juni 2013 publik gemacht hat. Ziele waren Firmen im Bereich Industrie, Energie, Telekommunikation und neue Technologien oder Regierungsstellen. Verschiedene Anhaltspunkte liessen Kaspersky im September 2013 auf eine Neuauflage dieser APT mit neuen Angriffsmethoden schliessen. Neu wurde zur Verbreitung der Malware neben dem bislang meist angewendeten Spearphishing die Watering-Hole-Methode verwendet.[34] Eine weitere Neuerung stellte FireEye mit der Nutzung einer Sicherheitslücke bei Java fest.

Einen weiteren APT «Operation Molerats» hat FireEye im Oktober 2012 aufgedeckt. Im Visier waren Regierungsziele in Israel und auch Palästina. Die Operation soll vom Mittleren Osten aus durchgeführt worden sein. Als Schadsoftware wurde «XtremeRAT» verwendet, eine verbreitete und oft mit Angreifern aus dieser Region in Verbindung gebrachte Malware. Neue Erkenntnisse von FireEye im August 2013 gehen davon aus, dass die gleiche Gruppe bei Angriffen in den USA und im Mittleren Osten auch Poison Ivy verwendet. Poison Ivy ist ebenfalls eine weitverbreitete und meist chinesischen Tätergruppen zugeschriebene Malware. Dass sie von Angreifern einer anderen geografischen Region verwendet werden, ist neu.

Die beiden Beispiele zeigen, wie anpassungs- und wandlungsfähig APT-Angreifer sind. Diese Gruppen verwenden immer neue, auf das Ziel und die Umstände abgestimmte Methoden. Das muss bei allen Analysen berücksichtigt werden.

Der Umstand ist insbesondere bei der Zuordnung der Angriffe zu beachten. Bei der Attribution müssen verschiedene Elemente berücksichtigt werden. Ein zu eindimensionaler Ansatz nur gestützt auf den Modus Operandi und die verwendeten Werkzeuge ist in der Regel riskant. Eine Attribution ist entsprechend auch auf nicht technische Informationen abzustützen, und es sind immer auch die eigentlichen Absichten, Motive, Opfer und Auswirkungen in Betracht zu ziehen.

---

[32] http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html?pagewanted=all (Stand: 20. Februar 2014).

[33] Siehe hierzu Kapitel 5.1 des aktuellen Berichtes.

[34] MELANI Halbjahresbericht 2013/1, Kapitel 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

4.3 Millionen von Adobe-Kundendaten gestohlen

Einer der grössten Passwort-Diebstähle ist Anfang Oktober bekannt geworden. Das Opfer war Adobe. Nachdem zuerst von 2.9 Millionen Kundendaten, Passwörtern und Kreditkartendaten die Rede war, korrigierte Adobe nach einigen Wochen die Zahl auf 38 Millionen.[35] Eine zusätzlich aufgetauchte 3.8 GB grosse Datei soll sogar 150 Millionen Nutzerdaten und *gehashte* Passwörter enthalten. Dies wurde jedoch von Adobe offiziell nicht bestätigt. Laut Adobe wurden verschlüsselte Kreditkartendaten und Passwörter gestohlen. Zur Entschlüsselung der Daten wird ein Sicherheitsschlüssel (*3DES*) benötigt, den die Angreifer voraussichtlich nicht stehlen konnten. Ohne Verschlüsselung einsehbar waren aber die Passworterinnerungen, über welche teilweise recht einfach auf die Passwörter geschlossen werden konnte. Beispielsweise lässt der Passworthinweis «1-6» auf die Zahlenkombination «123456» schliessen. Da immer der gleiche 3DES Schlüssel verwendet wurde, sahen alle identischen Passwörter auch nach der Verschlüsselung gleich aus und man konnte so identische Passörter zusammenfassen. Diese Hinweise genügten, um eine Liste mit den 100 meist verwendeten Passwörtern zu erstellen und diese zu publizieren.[36] Was dabei auffiel war, dass viele der Nutzer sehr einfache Passwörter gewählt haben. Dies kann zum Einen auf fehlende Sensibilisierung zurückzuführen sein, zum Anderen ist es möglich, dass Kunden gewisse Accounts und Passwörter als «wertlos» erachten, da sie beispielsweise das Konto nur für einen Einkauf benutzen wollen oder aber denken, dass sich in dem Konto keine schützenswerten Daten befinden.

Adobe hat nach dem Bekanntwerden des Angriffs alle Passwörter zurückgesetzt. Die 38 Millionen, die laut Adobe direkt betroffen waren, wurden via E-Mail informiert und zur Eingabe eines neuen Passwortes angehalten.

Zusätzlich zu Nutzerdaten soll es den Angreifern auch möglich gewesen sein, die *Sourcecodes* von Adobe ColdFusion, Acrobat und Photoshop Produkten zu beschaffen. Der Angriff soll sich im August 2013 ereignet haben.

Neben all den Unannehmlichkeiten, die ein solcher Fall für eine Firma mit sich bringt, ist die Kundenkommunikation ein wichtiges Element, um den Schaden so gering wie möglich zu halten. Adobe hat alle Passwörter zurückgesetzt, betroffene Kunden via E-Mail über den Angriff informiert und sie aufgefordert, ein neues Passwort zu wählen.

Gerade solche E-Mails müssen aber sehr überlegt versendet werden, da diese einerseits prädestiniert sind, als Vorlage für weitere (Phishing-)Angriffe zu dienen. Andererseits ist die Sensibilität von Internetbenutzern mittlerweile so hoch, dass solche E-Mails, die zum Passwortwechsel auffordern, schnell einmal als betrügerisch taxiert werden. So hat MELANI zahlreiche Meldungen von Bürgern erhalten, die skeptisch waren, ob diese Informations-E-Mail von Adobe auch tatsächlich von Adobe stamme. Eine allzu sorglose Kundenkommunikation durch eine Firma kann auch das Kundenverhalten bezüglich betrügerischen E-Mails negativ beeinflussen.[37]

Ein nicht zu unterschätzendes Problem in solchen Fällen ist, dass Benutzer ein Passwort nicht nur für einen Dienst, sondern für mehrere Dienste nutzen. Ist ein Passwort mit zugehöriger E-Mail-Adresse erst einmal gestohlen, ergeben sich so Möglichkeiten, auch auf andere Internet-Dienstleistungen zuzugreifen.

---

35 http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ (Stand: 20. Februar 2014).

36 http://stricture-group.com/files/adobe-top100.txt (Stand: 20. Februar 2014).

37 MELANI Halbjahresbericht 2012/1, Kapitel 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 20. Februar 2014).

4.4 Angriffe bei Target-Verkaufsstellen

Im Dezember berichteten verschiedene Medien von einem Grossangriff bei der Ladenkette Target. Target bestätigte diese Artikel mittels Medienmitteilung, dessen Informationen zufolge 40 Millionen Kreditkartenzahlungen und 70 Millionen Kundendaten gestohlen wurden.

Der Angriff erfolgte im intensiven Vorweihnachtsgeschäft zwischen 27. November und 15. Dezember. Target kommunizierte zuerst äusserst zurückhaltend über den Vorfall. Erst aufgrund von Recherchen und publik gewordenen Informationen aus verschiedenen Quellen konnten die Umstände und die Methoden des Angriffs teils nach und nach rekonstruiert werden. Etliche Aspekte sind aber zum Zeitpunkt der Redaktion dieses Berichts weiterhin unklar.

Laut ersten von Target bestätigten Analysen erfolgte der Einbruch über eine Malware in den Zahlungsterminals (*Point of Sales)* der Verkaufsstellen.[38] Dabei soll es sich um die Schadsoftware BlackPOS gehandelt haben, die angeblich durch kriminelle Banden aus Osteuropa implementiert worden sein soll, oder um eine seiner Varianten. Diese Malware liest die Daten auf dem Magnetband der Karte direkt nach der Verwendung im Zahlungsterminal, während sie in dessen RAM enthalten sind. Vor dieser unter dem Namen Ramscraping bekannten Methode hat unter anderem im letzten Sommer VISA schon gewarnt.[39] Auf die zentralen Fragen, welche Daten kopiert wurden und wo der Eintrittspunkts («Entry Point») war, wurden erst nach mehreren Wochen und nach diversen Bekanntgaben und Stellungnahmen Teilantworten geliefert. Target führte den Einbruch auf gestohlene Netzzugangsdaten bei einem Lieferanten zurück. Sukzessive verdichteten sich dann aber die Hinweise, dass es sich um die Wartungsfirma des Heizungs- und Klimaanlagensystems handelte, die als Eingangspunkt der Malware fungierte. Die Zugangsdaten sollen über E-Mail mit einer Passwort-Malware an die Firma erlangt worden sein. Via Berechtigungen des Lieferanten sollen dann die Angreifer Zugang zum Zahlungssystem bekommen und dort eine Malware zum Abfangen der Daten installiert haben.

Im Januar wurde ein ähnlicher Angriff bei der Ladenkette Neiman Marcus bekannt. Auch da wurden die Daten des Magnetbands unmittelbar nach Gebrauch abgefangen. In den beiden Fällen scheinen ähnliche Methoden zum Einsatz gekommen zu sein, ohne dass diese jedoch bisher mit Sicherheit der gleichen Täterschaft zugeschrieben werden konnten. Diversen Quellen zufolge sollen noch weitere, bisher aber nicht bekannt gewordene Läden betroffen sein.

Der Angriff bei Target und weitere ähnliche Fälle machen das Risiko eines blossen Magnetband-Kreditkartensystems deutlich. Dieses System, welches eine geringere Sicherheit bietet als Chip und PIN, ist in den USA noch weit verbreitet. Die Daten können dabei verhältnismässig leicht abgefangen werden. Meist werden sie dann auf spezialisierten Webseiten und Foren angeboten und letztlich für die Herstellung gefälschter Kreditkarten verwendet.

Der Vorfall weist auf eine weitere Problematik hin, nämlich die der externen Mitarbeiter, die im Netz eines Unternehmens arbeiten und über erweiterte Rechte verfügen. Wie das Beispiel zeigt, stellen auch sie potenzielle Einfallstore für Angreifer dar.

---

[38] Schwachstellen in POS wurden bereits im MELANI Halbjahresbericht 2012/2 thematisiert. MELANI Halbjahresbericht 2012/2, Kapitel 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (Stand: 20. Februar 2014).

[39] http://usa.visa.com/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf (Stand: 20. Februar 2014).

4.5 SIM-Zweitkarten und ihre Folgen

Angriffe auf Smartphones, welche das Ziel haben, mit *mTAN* gesicherte E-Banking Systeme anzugreifen, wurden bereits im letzten Halbjahresbericht[40] thematisiert. Das auch Angriffe möglich sind, die nicht technische, sondern organisatorische Schwachstellen ausnutzen, wurde Ende Oktober 2013 bewiesen. Damals gab es erste Berichte, dass es Betrügern in Deutschland gelungen war durch mTAN gesicherte E-Banking-Applikationen mittels zweiter *SIM* (Subscriber Identity Module)-*Karte* zu kompromittieren. Hierzu liessen sich die Betrüger einfach eine zweite SIM-Karte an eine beliebige Zweitadresse zustellen und konnten mit Hilfe dieser Karte die ankommenden mTAN mitlesen.

Eine SIM-Karte stellt die Autorisation des Benutzers sicher. Ist eine Person im Besitz dieser Karte, ist es prinzipiell möglich, sich im Namen des Benutzers in das Mobilfunknetz einzuwählen. Je nach Policy der Mobilfunkbetreiber ist ein paralleles Betreiben von mehreren SIM-Karten möglich. Wenn vom Telekomanbieter nur eine Karte akzeptiert wird, stören sich meist die beiden SIM Karten.

Neben dieser technischen Einschränkung stellt sich allerdings die organisatorische Frage, welche Sicherheitsmassnahmen Mobilfunkbetreiber bei der Abgabe von SIM Karten anwenden. Da immer häufiger auch kritische Dienstleistungen über das Mobiltelefon abgewickelt werden, gerät auch die Sicherheit dieser Mobilfunktelefone und auch der Mobilfunkbetreiber stärker in den Fokus.

4.6 Gehackter DES-Algorithmus und die Folgen für SIM-Karten

Der deutsche Kryptospezialist Karsten Nohl hat im Juli 2013 erste Resultate zu seinen Recherchen zur Sicherheit von SIM-Karten veröffentlicht. Danach sind mehrere Millionen SIM-Karten rund um die Welt ungenügend gesichert und können kompromittiert werden. Dies ermöglicht zum Beispiel einen Übergriff auf die Identität des Nutzers, Lauschangriffe oder auch Manipulationen von Zahlungen, welche über die Mobiltelefoninfrastruktur abgewickelt werden.[41]

Die Netze der Mobilfunkanbieter kommunizieren regelmässig mit den SIM-Karten, ohne dass deren Benutzer etwas davon merken. Genutzt wird eine Technologie, die es erlaubt, aus der Distanz an die Daten einer SIM-Karte zu gelangen («*Over-the-air*»-Technologie). Auf diese Weise werden beispielsweise Aktualisierungen installiert und verschiedene Informationen ausgetauscht. Die Sicherheit der Kommunikation zwischen der SIM-Karte und dem Netzbetreiber ist durch eine Verschlüsselung gesichert. Karsten Nohl stellt gerade diese Verschlüsselung in Frage. Konkret geht es um den «Data Encryption Standard» (DES), welcher bereits in den 1970er-Jahren entwickelt worden ist, aber immer noch in gewissen Applikationen verwendet wird. Der DES-Algorithmus gilt seit langem als wenig sicher, insbesondere wegen der ungenügenden Länge der eingesetzten Schlüssel von 56 Bit. Laut Nohl ist es möglich, den kryptografischen Schlüssel von gewissen SIM-Karten mit DES-Verschlüsselung herauszufinden.

---

[40] MELANI Halbjahresbericht 2013/1, Kapitel 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

[41] https://srlabs.de/rooting-sim-cards/ (Stand: 20. Februar 2014).
http://www.heise.de/security/artikel/DES-Hack-exponiert-Millionen-SIM-Karten-1920898.html (Stand: 20. Februar 2014).

Ist der Hacker erst einmal im Besitz dieses Schlüssels, hat er auch die Möglichkeit, verschiedene Angriffe gegen die SIM-Karte und deren Besitzer zu lancieren. Basierend auf dieser Sicherheitslücke hat Nohl erfolgreich einen Viertel der getesteten SIM-Karten gehackt. Es wird angenommen, dass weltweit noch ungefähr 500 Millionen SIM-Karten diesem Risiko ausgesetzt sind. Neuere SIM-Karten, welche die Nachfolger des DES verwenden, sind auf diese Weise nicht angreifbar.

Die publizierte Sicherheitslücke verfügt über ein grosses Schadenspotenzial für Benutzer einer durch die DES-Methode geschützten SIM-Karte. Für den Schweizer Markt besteht allerdings keine Gefahr. Gemäss Informationen, die MELANI von den Schweizer Telekommunikationsunternehmen erhalten hat, wird der DES-Standard in der Schweiz nicht mehr eingesetzt.

4.7 Industrielle und private Kontrollsysteme

Vernetzte Industrieanlagen und ferngesteuerte Hausanlagen

Mehrfach hat MELANI bereits auf die Risiken der zunehmenden Vernetzung von Steuerungsgeräten physischer Prozesse im industriellen wie auch im privaten Bereich hingewiesen.[42] Durch die technische Entwicklung werden stets mehr Möglichkeiten erschlossen, aus der Ferne auf Systeme zuzugreifen, Daten abzufragen und schliesslich auch dahinterliegende Geräte zu steuern. Und mittlerweile ist es relativ einfach und günstig, Systeme mit Fernabfrage- und –steuerungsfunktion zu beziehen oder eine bestehende Anlage mit einer Kommunikationsschnittstelle nachzurüsten. Dies entspricht häufig den Kundenwünschen: Es ist praktisch und angenehm, auf dem Weg ins Ferienhaus via Tablet-Computer oder Smartphone die Heizung und den Boiler anzuschalten oder überprüfen zu können, ob man zuhause den Herd abgeschaltet hat. Dies gilt ebenso für Liegenschaftsbetreuer, die durch den Fernzugriff die Systeme der Hausautomation überwachen und steuern können. Auch Betreiber von kleinen Wasserkraftwerken oder anderen Anlagen, die nicht rund um die Uhr besetzt sind, schätzen es, vom heimischen Sofa aus das Funktionieren zu überprüfen und gewisse Einstellungen vornehmen zu können.

Auf jedes System, das legitimen *Fernzugang* erlaubt, kann grundsätzlich auch unberechtigt zugegriffen werden, sei dies direkt oder durch Infiltration eines zugangsberechtigten Geräts, denn es gilt nach wie vor «Alles was über das Netz erreichbar ist, ist hackbar.»[43] Die Vernetzung von industriellen Kontrollsystemen und die IKT-Steuerung der Hausautomation weckt zunehmend das Interesse von Sicherheitsexperten. So wurden in den letzten Jahren verschiedene Sicherheitslücken in solchen Produkten oder bei deren Implementierung identifiziert.[44]

Die verschiedenen fernsteuerbaren Systeme erfüllen diverse Aufgaben und allfällige Manipulationen haben unterschiedliche Konsequenzen für die Betroffenen: Wird ein Boiler ausgeschaltet, können die Hausbewohner nur kalt duschen; das Einschalten der Flutlichtanlage in einem Stadion kostet Strom und Geld; wird eine industrielle Produktionsstrasse angehalten, kommt vielleicht der ganze Betrieb zum Stillstand, was für das Unternehmen und die Angestellten weitreichende Konsequenzen haben kann.

---

[42] Zum Beispiel: MELANI Halbjahresbericht 2013/1, Kapitel 4.5: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

[43] «If you can ping it, you own it!» Kyle Wilhoit, The SCADA That Didn't Cry Wolf, 2013.

[44] http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities (Stand: 20. Februar 2014).

Schliesslich ist auch ein Szenario vorstellbar, bei welchem viele Verbrauchergeräte koordiniert ein- oder ausgeschaltet werden und dadurch die Stabilität des Stromnetzes gefährdet würde. Entsprechend ist neben Funktion und Benutzerfreundlichkeit einer Fernzugangslösung auch dem Schutz vor unbefugten Manipulationen Beachtung zu schenken.

Zwar soll die IKT in erster Linie betriebliche Prozesse unterstützen. Doch der Einsatz von IKT hat immer auch physische und prozedurale Auswirkungen welche berücksichtigt werden müssen.

MELANI hat im Oktober 2013 eine Checkliste zum Schutz von industriellen Kontrollsystemen publiziert.[45]

«Good Practices» der OSZE zur Reduzierung von Cyber-Risiken im Energiesektor

Die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) hat eine Anleitung für Staaten und private Energieunternehmen publiziert, wie diese ihre Infrastrukturen vor möglichen cyber-terroristischen Anschlägen schützen können.[46] Obschon der Titel des Dokuments einen relativ engen Fokus suggeriert, führt es von einer breiten Sicht an das Thema heran und empfiehlt generelle Massnahmen, die gleichwohl auf weitere Industriebereiche angewendet werden können und nicht nur gegen terroristische Anschläge präventiv und resilienzsteigernd wirken. Die OSZE plädiert für die Förderung von Bewusstsein (Awareness Rising) durch Schulungen, für vermehrte Kooperation aller Beteiligten und Informationsaustausch. Diese Massnahmen werden von vielen Seiten propagiert und nun von der OSZE besonders für den nicht-nuklearen Energiesektor aufgezeigt. Die Kernenergie wurde wohl deshalb ausgeklammert, um keine Kompetenzstreitigkeiten mit den entsprechenden Regulatoren zu provozieren – die Empfehlungen der OSZE sind jedoch auch für Betreiber von Kernanlagen beachtenswert.

Für die stark fragmentierte, jedoch immer stärker vernetzte Energieversorgung Europas liegt es in der gemeinsamen Verantwortung aller Beteiligten, die Versorgungssicherheit zu gewährleisten. Viele andere Sektoren sind von der Energieversorgung, insbesondere von der Elektrizität abhängig. Dies lässt die Stromversorgung als besonders kritisch erscheinen. Hinzu kommt die Entwicklung hin zu intelligenten Stromnetzen, welche die Risiken zusätzlich erhöhen: Die durch IKT gesteuerten zusätzlichen Mess- und Regelstellen bringen neben neuen komfortablen Möglichkeiten für die Versorger auch neue Angriffsflächen für böswillige Akteure mit sich, die darüber in die Stromversorgung eingreifen können. Entsprechend ist der Sicherheit von «intelligenten» Komponenten bei der Energieversorgung gebührend Rechnung zu tragen.

4.8 Der Syrien-Konflikt – Informationskrieg 2.0

Die Syrian Electronic Army (SEA) ist eine Gruppe von Hackern, die das Regime um den syrischen Präsidenten Bashar al-Asad unterstützen. Die Verbindungen zwischen der SEA und der syrischen Führung sind jedoch nicht klar. Gemäss eigenen Aussagen der SEA sei sie nicht Teil der Regierung und werde durch diese auch nicht unterstützt. Sie bestehe vielmehr aus patriotischen Hackern, welche gegen – aus ihrer Sicht – falsche Berichterstattung über den syrischen Bürgerkrieg kämpfen.

[45] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=de (Stand: 20. Februar 2014).

[46] «Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace», http://www.osce.org/atu/103500 (Stand: 20. Februar 2014).

Die SEA griff im letzten Halbjahr vor allem Nachrichtenwebseiten an (New York Times, BBC News, Al-Jazeera u.a.) und konnte unter anderem sogar die Twitter-Konten von Nachrichtenagenturen wie Reuters und Associated Press (AP) kompromittieren mit dem Ziel, ihre eigene Propaganda oder bewusste Falschmeldungen zu verbreiten.[47]

Schon vor über zweitausend Jahren bemerkte der griechische Dichter Aischylos: «Im Krieg ist die Wahrheit das erste Opfer.» Mit dem Aufkommen des Internet und insbesondere der Sozialen Medien wurde die Informationskriegsführung nun «demokratisiert». Es braucht nicht zwingend mehr staatliche Interventionen, um (falsche oder korrekte) Informationen in die Welt zu setzen – man benötigt nur einen Internetanschluss und eine Geschichte, welche sich viral verbreiten kann.

Social-Media-Konten und andere Informationskanäle, die den Zugang und anschliessende Informationsverbreitung nur durch Benutzernamen und Passwort authentisieren, sind mit Methoden wie *Spear-Phishing* relativ einfach zu infiltrieren. Wichtige Informationskanäle und -plattformen sollten deshalb möglichst durch eine *Zwei-Faktor-Authentisierung* geschützt werden.

Neben technischen Massnahmen sollte zudem im Vorfeld überlegt und definiert werden, wie und über welche Kanäle eine Falschmeldung möglichst effizient dementiert, respektive richtiggestellt werden kann, um damit grössere Verwirrung und andere Auswirkungen zu verhindern.

4.9 Wenn DDoS von anderen Angriffen ablenkt

Ein Trend im letzten Jahr waren DDoS (Distributed Denial of Service) Angriffe von geringer Intensität, welche von anderen Angriffen abzulenken versuchen. Verschiedene Experten und Artikel haben über das Phänomen berichtet, das offenbar vor allem amerikanische Banken betraf. Während die Sicherheitsverantwortlichen damit beschäftigt waren, die DDoS auf die Firmenwebseite oder das E-Banking-Portal abzuwenden, erfolgt parallel ein anderer Angriff. Im Fokus standen dabei nicht primär einzelne Konten, sondern das gesamte Überweisungssystem der Bank. Zusätzlich wird die Auswertung des Vorfalls durch die grosse Menge an Logdaten erschwert.

Es ist klar, dass bei einem DDoS-Angriff dieser als solcher bearbeitet und auch abgewehrt werden muss, gleichzeitig sollte ein solcher Angriff auch die Sensibilität gegenüber potenzieller Parallelangriffe erhöhen. Das gilt besonders bei DDoS-Angriffen niedriger Intensität.

4.10 Hacker und Schmuggler unter einer Decke

Im Hafen von Antwerpen sind zwischen 2011 und 2013 mehrere Schiffscontainer «verschwunden». Ermittlungen der Strafverfolgungsbehörden ergaben, dass die legalen Container von Kriminellen missbraucht wurden, um Drogen zu schmuggeln. Zu diesem Zweck schleusten sich die Täter in die IKT-Systeme von Container-Unternehmen ein, um so die Standorte der betroffenen Container ausfindig zu machen und diese zu stehlen, bevor die rechtmässigen Eigentümer sie abholen konnten.

---

[47] Siehe dazu bereits Kapitel 4.4 im letzten MELANI-Halbjahresbericht: HJB 2013/I, Kap. 4.4. http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

Das ursprüngliche Eindringen in die Informationssysteme wurde durch einfache «*Social Engineering*»-E-Mails bewerkstelligt, mit welchen Firmenangestellte zum Öffnen von *Attachments* und damit zur Installation von Spionageprogrammen verleitet wurden. Nach der Entdeckung dieser Vorfälle wurden die (IKT-)Sicherheitsmassnahmen bei den Container-Unternehmen verstärkt. Die Täter verschafften sich daraufhin physischen Zugang zu den Büros und installierten manipulierte Hardware, um weiterhin Zugang zu den benötigten Informationen zu erhalten – unter anderem die Sicherheitscodes, die den Fahrern den Zugang zum Gelände und die Abholung bestimmter Container erlaubte.

Die Informatikinfrastruktur, welche die Planung und Ausführung von Geschäftstätigkeiten unterstützt, ist in vielen Bereichen nicht mehr wegzudenken. Insbesondere anspruchsvolle logistische Aufgaben lassen sich ohne Informatiksysteme kaum mehr bewerkstelligen. Zudem wünschen sich viele Logistik-Unternehmen, jederzeit den aktuellen Standort von Lieferungen und Transportmitteln eruieren zu können. Diese Informationen, welche eine effizientere Ressourcennutzung und Leistungserbringung ermöglichen, bieten gleichzeitig die Möglichkeiten für gezielte kriminelle Aktionen. Weiter ist zu bedenken, dass Manipulationen dieser Informationen den regulären Geschäftsgang beeinträchtigen können. Dennoch sind IKT-Systeme in erster Linie ein weiteres Mittel zur Unterstützung von bestimmten betrieblichen Abläufen. Somit ist auf Geschäftsleitungsebene in erster Linie das Verständnis für die physischen und prozeduralen Auswirkungen solcher Systeme massgebend.

Wie in jedem Markt zeichnet sich auch im Untergrundmarkt des Internet eine zunehmende Spezialisierung und Professionalisierung ab. Diese Tendenz ist seit einigen Jahren zu beobachten. Bei Hackern handelt es sich nicht mehr nur um neugierige Jugendliche, welche die Grenzen des Möglichen austesten möchten, sondern vermehrt um erfahrene Techniker, welche ihre Fähigkeiten profitorientiert anbieten. Auch im vorliegenden Fall wurden die Hacker von den Schmugglern scheinbar via Internet rekrutiert. Es gibt kaum eine Dienstleistung, welche nicht im Untergrundmarkt des Internet bezogen werden kann.

4.11 EU-Parlament verabschiedet härtere Strafen für Cyberkriminelle

Cyberkriminellen drohen künftig in der Europäischen Union höhere Strafen. Mit der Verabschiedung der Richtlinie 2013/40/EU hat das Europäische Parlament am 12. August 2013 härtere Strafen bei Angriffen auf Informationssysteme beschlossen. Ziel ist unter anderem eine Gesetzes- und Strafharmonisierung unter den Mitgliederstaaten zu erreichen, da Angriffe und Betrügereien oft länderübergreifend stattfinden und diese Taten in den EU-Staaten unterschiedlich geahndet werden. Die Vereinheitlichung des Strafrahmens schafft die nötige Grundlage zur Zusammenarbeit in der Strafverfolgung.

Die Richtlinie sieht Haftstrafen von mindestens zwei Jahren vor. So wird beispielsweise das Aufbauen von *Botnetzen* mit mindestens drei Jahren Gefängnis geahndet. Kriminellen, die für Angriffe auf kritische Infrastrukturen wie Kraftwerke, Transportsysteme oder Regierungsnetzwerke verantwortlich sind, drohen mindestens fünf Jahre Gefängnis. Dasselbe gilt, wenn ein Angriff nicht von einer Einzelperson, sondern von einer kriminellen Vereinigung durchgeführt worden ist oder wenn schwere Schäden verursacht werden.

Die Richtlinie enthält zusätzlich Auflagen für die Polizei und Justizbehörden. So sollen die EU-Mitgliedstaaten Informationen über Cyberangriffe austauschen, um den Betrieb der Netze sicherzustellen. Um den Informationsaustausch zusätzlich zu verbessern, sollen die zuständigen Stellen innerhalb von acht Stunden auf dringende Anfragen reagieren.

Diesem neuen Kurs liegt in erster Linie das Ziel einer ansatzmässigen Harmonisierung der strafrechtlichen Grundlage im Bereich Cyberkriminalität in den EU-Staaten zugrunde. Die Praxis hat gezeigt, dass die Strafverfolgung bei grenzüberschreitender Cyber-Kriminalität regelmässig an formale Grenzen stösst, welche auf unterschiedliche Ansätze des Strafprozesses der Mitgliedstaaten zurückzuführen sind. Ob sich die höheren Strafandrohungen in Zukunft umsetzen lassen, wird im Wesentlichen davon abhängen, wie dieser gemeinsame Rahmen in den nationalen Gesetzen der Mitgliedstaaten verankert wird.

5 Tendenzen / Ausblick

5.1 Das Internet am Scheideweg oder Business as usual?

Mit der fortgesetzten Veröffentlichung von Dokumenten zur Praxis der NSA und anderer Nachrichtendienste wurden in den letzten Monaten auch Stimmen laut, die sich zur Zukunft des Internets als solches äusserten. Dabei gehen die diversen Einschätzungen erwartungsgemäss in alle Richtungen: So beklagt der Sicherheitsexperte Bruce Schneier in einem seiner Artikel den fundamentalen Verrat am Internet und den Grundwerten für die es stehe.[48] Er unterstreicht dabei auch das Paradoxon, dass gerade die Aktionen der USA - dem Anführer der freien Welt – nun die Absichten jener totalitären Staaten bekräftigen, die schon immer eine Nationalisierung des Internets anstrebten. Diese Furcht vor einer zunehmenden «Balkanisierung des Internets» treibt beispielsweise den Google Vizepräsidenten, Vinton Cerf, dazu, bereits den Untergang des Internets, wie man es heute kennt, heraufzubeschwören.[49] Mit einer zunehmenden nationalen Abschottung und einer damit einhergehenden Heterogenisierung des Marktes werde es wirtschaftlich für Unternehmen nicht mehr interessant sein, am Internet teilzuhaben. Auch aus der Ecke der Anhänger, für die das Internet die basisdemokratische und freiheitsbringende Erfindung schlecht hin ist, kommen kritische Stimmen. Sie begreifen das Internet nun eher als die perfekte Überwachungsplattform und werfen sich die eigene Naivität vor, jemals überhaupt etwas anderes darin gesehen zu haben.

Gleichzeitig aber scheint das Internet noch immer sehr lebendig zu sein und zumindest kurzfristig wird sich an diesem Zustand wohl auch nichts ändern. Die durch die Snowden-Dokumente bekannt gewordenen Aktivitäten einzelner Nachrichtendienste lassen aber zumindest den Schluss zu, dass das Vertrauen ins Internet gerade auf mehreren Ebenen wohl endgültig verloren ist.

Sie zeigen aber auch die eklatanten Probleme auf, die eine solch transnationale Einrichtung mit sich bringt, an der jedes Individuum, jeder Staat so teilhaben kann und machen darf, wie es ihm gerade beliebt und die nationalen Gesetze es zulassen, ohne dabei auf die globalen Auswirkungen Rücksicht nehmen zu müssen. Wenn auf technischer Ebene von einem einzelnen Land die globalen Sicherheitsstandards nach eigenem Gutdünken verändert werden oder die eigenen Unternehmen mit geheimen Zwangsmassnahmen aufgefordert werden, Informationen in grossem Stil auszuhändigen, um im Interesse der nationalen Sicherheit, möglichst einfach und flächendeckend an Daten heranzukommen, so mag das gegen Treu und Glaube verstossen und wohl auch gegen eine Vielzahl anderer nationaler Rechtswerke.

---

[48] http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying (Stand: 20. Februar 2014).

[49] http://www.tagesanzeiger.ch/digital/internet/GoogleVize-warnt-vor-Untergang-des-Internets/story/12499111 (Stand: 20. Februar 2014).

Es macht den Staatsangestellten die Erreichung ihrer Ziele aber um Einiges leichter und angenehmer. Scheinbar vergessen geht dabei, dass Gier gepaart mit Faulheit bei der staatlichen Beschaffung von Informationen und Personendaten unter liberalen, demokratischen Gesichtspunkten zumindest immer grenzwertige Ansätze sind.

Gerade für Unternehmen im IT-Bereich heisst das, dass sie zwar in einem globalen Umfeld agieren, am Ende aber unterschiedlichen, sich nicht immer entsprechenden nationalen Rechtsgrundlagen ausgesetzt sind. Das gilt dabei nicht nur für jene Unternehmen, die im IT-Bereich tätig sind. Ein Hauptthema muss daher sein, gerade dieses Fehlen eines Konsenses zu fundamentale Prinzipien im Umgang mit dem Internet und den beteiligten Akteuren anzugehen.

Verknüpft mit diesen Fragen ist auch der Wiederaufbau des Vertrauens gerade in der IT-Sicherheitsgemeinschaft. Also das Vertrauen und den internationalen Austausch zwischen jenen IT-Sicherheitsorganen, die in erster Linie darauf ausgerichtet sind Netzwerke, Produkte und Anwendungen zu schützen. Dass beispielsweise das bei Sicherheitsstandards führende «Directorate for Information Assurance» in den USA dem Chef der NSA unterstellt ist, welcher sich auf Grund seines Pflichtenheftes wohl nicht ausschliesslich für sichere IT-Produkten und robuste Standards interessieren dürfte, ist nur eine Komplizierung in diesem Zusammenhang. Auch die Ansiedelung von im internationalen Informationsaustausch zur Sicherung der Netzwerk eingebundenen Regierungs-Certs bei offensiven «Signal Intelligence» Einheiten, unterstützt das Vertrauen anderer Regierungs-Certs wohl nur bedingt. Allerdings ist es gerade diese technische Community und ihr länderübergreifendes System des Informationsaustausches, welche wohl einen Bärenteil der Aufgabe übernehmen muss, das Internet, respektive die Sicherheit seiner Komponenten, wieder so auf Vordermann zu bringen, damit eine weitere Abschottung vermieden und das Grundvertrauen ins Internet wieder repariert werden kann.

Das Internet in seinem rund 25. Lebensjahr bereits dem Tod zu weihen, geht wohl zu weit. Allerdings steht mit dem Weideraufbau des Grundvertrauens in das Internet, sowie dem Vertrauen der sicherheitsrelevanten Akteure im IKT-Bereich untereinander eine nicht ganz triviale Aufgabe an. Auch die Lösung der Grundfrage, wie damit umgegangen werden soll, dass bei einer Anwendung von Landesrecht in einem transnationalen System wie dem Internet immer auch eine de facto extraterritoriale Auswirkung der Rechtsanwendung folgt, wird keine einfache Antworten mit sich bringen. Vor allem wird sich diese Diskussion über alle Ebenen hindurchziehen müssen, von der sicherheitspolitischen Sicht, bis zu den Multi-Stake-Holder Gremien, die sich mit Standards und Auflagen befassen und in denen auch die Wirtschaft als Hauptbetroffene einsitzt.

In jedem Falle angesagt ist aber eine Bestandsaufnahme und Rückbesinnung auf die Grundidee, die das Internet dargestellt hat: In erster Linie ein höchst widerstandsfähiges, dezentrales System zu sein, um darauf Informationen zu übermitteln. Die Sicherheit und Vertraulichkeit dieser Informationen war dabei nie oder zumindest nur am Rande in diese Vision integriert. Sicherheit und Vertraulichkeit lagen, liegen und werden auch in Zukunft in der Verantwortung jener liegen, die diese Informationen und Daten dem Internet überhaupt erst zuführen.

5.2 Bitcoin - der Erfolg und sein Preis

Funktionsweise

Bitcoin ist eine dezentrale digitale Währung, das heisst sie hängt von keiner zentralen Ausgabestelle ab. Dadurch unterscheidet sie sich nicht nur von den traditionellen, sondern auch von anderen digitalen Währungen.

Bitcoin hat zwei Arten von Hauptakteuren. Die Benutzer sind mit ihrem «Wallet» (ihrer Brieftasche) vertreten, welches aus einem öffentlichen und privaten Schlüsselpaar besteht. Der öffentliche Schlüssel entspricht sinngemäss der Nummer des Kontos, auf das man Geld transferieren kann. Mit dem privaten Schlüssel wird eine Transaktion signiert, das heisst eine Zahlung vorgenommen.

Bevor die Zahlung erfolgt, muss sie bestätigt werden. Bei diesem Prozess kommen als zweite Hauptakteure die so genannten Bitcoin-Miners, die «Mineure» ins Spiel. Sie tragen zum Aufbau der «Blockkette», dem Grundpfeiler des Systems bei. Bei der Blockkettte handelt es sich um eine Art allgemeines Kontobuch mit allen verifizierten Transaktionen. Beim Verifizierungsprozess, dem so genannten Mining, werden die aufgegebenen Transaktionen bestätigt und in einen Block aufgenommen. Die Validierung eines Blocks wird durch einen Mineur mit einem «Proof of Work». ausgelöst. Die dabei erforderlichen grossen Rechnerkapazitäten werden in Bitcoin entschädigt. Dadurch wird die Geldmenge im Umlauf erhöht. Die Integrität der Blockkette ist ein zentraler Punkt. Eine Transaktion darf nur erfolgen, wenn sie einem zuvor registrierten Eingang beim Auftraggeber entspricht. Sonst könnten Nutzer Transaktionen signieren, die keinerlei Bezug zur Realität haben.

Erworben werden Bitcoins hauptsächlich auf drei Arten: Durch Mitwirkung am Mining, indem man sich eine Leistung in Bitcoins bezahlen lässt, oder durch den Ankauf auf einer Handelsplattform, auf der Bitcoins gegen «klassische» Devisen getauscht werden. Anschliessend können die Bitcoins in Geschäften, die sie als Zahlungsmittel akzeptieren, eingesetzt werden. Es wird oft auf die Anonymität von Bitcoin-Transaktionen verwiesen. Dazu ist zu sagen, dass der Nutzer theoretisch anonym ist, da er nur über einen kryptografischen Schlüssel identifizierbar ist. Die Transaktionen hingegen sind anders als beim klassischen Bankensystem öffentlich.

Sicherheitsfragen

Mit zunehmender Popularität von Bitcoin stellen sich Fragen insbesondere in Bezug auf das Sicherheitsniveau, aber auch den Rechtsstatus und die Regulierung dieser Devisen.

Mehrere Vorfälle haben gezeigt, dass Kriminelle mehr und mehr Interesse an Bitcoins und ihren Nutzern zeigen und mit verschiedenen Methoden auch Bitcoins ergaunert haben. So wurden in den vergangenen Monaten diverse Attacken und Sicherheitsvorfälle mit unterschiedlichen Zielen und von unterschiedlicher Komplexität registriert.

Der private Schlüssel der Walletbesitzer ist in der Regel das attraktivste Ziel der Angreifer. Er allein gewährleistet die Sicherheit des Wallet und muss entsprechend sicher aufbewahrt werden. Viele Nutzer waren Opfer von Angriffen dieser Art. Zur Aufbewahrung der Schlüssel bieten deshalb Webdienste Ihren Kunden Speichermöglichkeiten an. Durch die dortige Konzentration von Wallets mit entsprechenden Summen haben sie sich als Hauptziele der Attacken erwiesen. Bei einem dieser Webdienste «input.io» wurden beispielsweise im Juli 2013 Bitcoins in der Höhe von 1.2 Millionen Dollar gestohlen.

Ein weiteres potenzielles Ziel sind die Handelsportale. Im Dezember gab der Devisenmarkt Bitcoin Schweiz bekannt, Opfer eines Angriffs geworden zu sein. Trotz rudimentärer Attacke, welche auf «Social Engineering» beruhte, war diese dennoch erfolgreich. Die Angreifer hatten sich als Bitcoin Schweiz ausgegeben und beim Mailprovider der Plattform die Änderung der Passwörter verlangt. Dieser kam der Aufforderung nach. Bitcoin Schweiz hat den Provider seither gewechselt. Ob die Angreifer die erbeuteten Daten für illegale Aktivitäten benutzt haben, wurde nicht bekanntgegeben. Es wurden auch weitere Arten von Angriffen beobachtet. Als Trend zeichnen sich DDoS-Angriffe ab. In einigen Fällen haben die Angreifer nach bekanntem Vorgehen mit Hilfe von DDoS-Angriffen Geld erpresst. Andere Angriffe haben es auf weitere Ziele abgesehen. Beispielsweise wurden gewisse Vorgänge beobachtet, welche

eine Destabilisierung des Marktes und einen sinkenden Kurs beabsichtigten, damit Bitcoins billiger erworben werden konnten. Im Zentrum steht hier die Kursvolatilität.

Ein weiteres Ziel sind die Entlohnungen für Miningaktivitäten. Anfang Jahr wurde eine über Werbung übertragene Malware auf verschiedenen Yahoo-Seiten entdeckt. Diese zapfte die die Rechnerkapazität der Opfersysteme an, um sie im Verborgenen Miningarbeiten ausführen zu lassen und damit Bitcoins zu erlangen.

Neben den Angriffen macht Bitcoin auch regelmässig von sich reden, weil es für illegale Transaktionen verwendet wird. So dient es weitgehend für Transaktionen auf Plattformen, die illegale Produkte anbieten wie beispielsweise Silk Road, eine E-Commerce-Plattform, die für Schwarzmarktaktivitäten verwendet wird.

Auch hier wird die grosse Anpassungsfähigkeit der Täter deutlich, die im Internet am Werk sind. Hat eine Idee wie das Zahlungsmittel Bitcoin Erfolg, lassen entsprechende Angriffe nicht lange auf sich warten. Dieses Risikos und der Anforderungen an die sichere Aufbewahrung der Bitcoins muss man sich auf Nutzerebene bewusst sein. Empfohlen wird dabei die Aufbewahrung des kryptografischen Schlüssels auf einem elektronischen Datenträger, zu dem kein Internetzugang besteht, oder auf Papier (Paperwallet). Darüber hinaus erweist sich auch hier die Sicherheit der Infrastruktur allgemein, insbesondere der Virenschutz, als zentral.

Der Rechtsrahmen und die Regulierung der Bitcoins sind erst im Aufbau. Durch die Popularität dieses Zahlungsmittels befassen sich die Staaten heute vermehrt mit den Missbrauchs- und Volatilitätsrisiken und ziehen Regelungen in Betracht. So wurde Bitcoin in Deutschland offiziell zur «privaten Währung» erklärt. In der Schweiz beschäftigten sich Ende letztes Jahr drei Parlamentsgeschäfte mit dem System oder genauer den Risiken und Chancen in Bezug auf einen möglichen Rechtsstatus.

5.3 Die Rolle von Cyber bei Konflikten

Bei vielen Konflikten spielt die Cyberkomponente mittlerweile eine Rolle, wie beispielsweise aktuell das Beispiel der Syrien Electronic Army im Syrien Konflikt zeigt.[50] Vor allem Propaganda und Desinformation werden hierbei beobachtet aber auch direkte Angriffe auf Infrastrukturen werden verzeichnet. Gern zitierte Beispiele sind der DDoS-Angriff auf Estland, die DDoS-Angriffe auf die US-Banken sowie die Angriffe in Süd- und Nordkorea. Immer wieder werden dann allerdings die Begriffe Cyberwar und Cyberterror verwendet, was in Anbetracht des tatsächlich entstandenen Schadens als unangebracht erscheint. So denkt man bei einem Terroranschlag oder Krieg unweigerlich an Panik, Angst und an Verletzte oder Tote. Cyberangriffe bewirkten bislang hingegen etwas ganz anderes: Nämlich Systemausfälle, Unannehmlichkeiten und Geldverluste.

Einsatz von Cyberangriffen besonders unter der Konfliktschwelle

Die Geschichte zeigt, dass Cyberangriffe gerade dann verwendet werden, wenn gezielt und unterhalb der Konfliktschwelle Operationen durchgeführt werden sollen, die, wenn konventionell geführt, zu erheblichen Zerwürfnissen zwischen Staaten führen würden. Ein typisches Beispiel ist der Einsatz der Schadsoftware Stuxnet, der zum Ziel hatte, die

[50] Aktueller MELANI Halbjahresbericht 2013/2, Kapitel 4.8
sowie MELANI Halbjahresbericht 2013/1, Kapitel 4.4:
http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 20. Februar 2014).

Zentrifugen in iranischen Urananreicherungsanlagen zu stören. Ein solcher mit konventionellen Mitteln durchgeführter Eingriff hätte wahrscheinlich zu einem ernsthaften Konflikt in der Region geführt.

Viele Akteure und Motivationen

Die Vielzahl der Akteure und Motivationen erschwert die Einschätzung zusätzlich. Ein DDoS Angriff auf eine Bank kann entweder einen kriminellen Hintergrund (Erpressung) oder einen ideologischen Hintergrund haben, wie beispielsweise die diversen Angriffe von Anonymous auf Banken in den letzten Jahren gezeigt haben. Aber auch ein staatlicher Hintergrund ist durchaus denkbar, wenn beispielsweise versucht würde, mit einem Angriff ein gesamtes Finanzsystem zu schwächen.

Die Beantwortung der Frage der Attribution dürfte in Zukunft noch schwieriger werden, da das enorme Potenzial von Personen mit Cyberfähigkeiten – unter anderem auch aus dem kriminellen Umfeld – von diversen Staaten erkannt und für ihre Zwecke verwendet werden wird. So können Aktionen in Auftrag gegeben und durchgeführt werden, ohne dass sich der Staat der Gefährdung einer Attribution aussetzen muss.

Zukünftige Angriffe

Ist die Gefahr von Cyberangriffen mit grossem Schadenspotenzial also gering? Natürlich besteht die Möglichkeit, dass auch besonders kritische Systeme angegriffen werden, deren Ausfall erhebliche Konsequenzen hätte. Allerdings verlangen solche Angriffe meist ein vertieftes Fach- und Insiderwissen, sowie bedeutenden Aufwand. Bei kritischen Systemen ist zudem das Augenmerk auf die Sicherheit besonders hoch. So sind es nicht ausschliesslich die Risiken von Cyberangriffen, welche zum Nachdenken anregen sollten, sondern insbesondere auch die Tatsache, dass Systeme immer komplizierter und vernetzter werden. Dadurch sind Verbindungen und Abhängigkeiten nicht mehr einfach zu erfassen. Ein Problem oder eine Störung kann so unvorhersehbare Auswirkungen nach sich ziehen. Es muss sich dabei nicht einmal um einen Angriff handeln – auch Pannen können hier für grössere Auswirkungen sorgen, und die Fehlersuche in einem komplexen System nimmt häufig einige Zeit in Anspruch.

5.4 Virendetektion im 21. Jahrhundert - Was kommt nach den signaturbasierten Antivirenprogrammen?

Die Geschichte der Virendetektion

Bereits im Jahr 1971 wurde der erste *Virus* beobachtet. Es handelte sich um Creeper, der sich innerhalb des Advanced Research Projects Agency Network, *ARPANET*, dem Vorläufer des heutigen Internets, verbreitete. Creeper wiederum wurde dann von einem «The Reaper» genannten Code bekämpft. Auch wenn der Begriff «Virus» damals noch nicht verwendet worden ist, kann «The Reaper» als erster Anti-Virus der Geschichte bezeichnet werden. Inzwischen bestehen seit über zwanzig Jahren kommerzielle Antiviren-Lösungen und es hat sich eine beachtliche Antiviren-Industrie entwickelt. Doch wo befindet sich diese Industrie im Moment und welche Abwehrmöglichkeiten haben aktuelle Antiviren-Produkte wirklich?

In einem 2012 publizierten Testbericht von «AV-Comparatives.org» ist der Prozentsatz der erfolgreich blockierten Schadsoftware respektive der erfolgreich blockierten schädlichen Webseiten erstaunlich hoch. Die Erkennungsrate beträgt hier über 90%:

Whole Product Dynamic "Real-World" Protection Test – (March-June) 2012 www.av-comparatives.org

Summary Results (March-June)

Test period: March – June 2012 (2159 Test cases)

	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][4]	Cluster[5]
BitDefender	2150	-	9	99,6%	1
G DATA	2147	1	11	99,5%	1
Kaspersky	2146	2	11	99,4%	1
Qihoo	2143	6	10	99,4%	1
BullGuard	2131	21	7	99,2%	1
F-Secure	2135	10	14	99,1%	1
Avast	2110	28	21	98,4%	2
ESET	2117	1	41	98,1%	2
AVIRA	2107	13	39	97,9%	2
Sophos	2112	-	47	97,8%	2
Trend Micro	2108	-	51	97,6%	2
AVG	2103	6	50	97,5%	2
GFI	2102	-	57	97,4%	2
Panda	2097	-	62	97,1%	2
eScan	2094	-	65	97,0%	2
PC Tools	2024	126	9	96,7%	2
Tencent	2052	32	75	95,8%	3
Fortinet	2046	-	113	94,8%	3
McAfee	2041	6	112	94,7%	3
AhnLab	1999	-	160	92,6%	4
Webroot	1963	1	195	90,9%	4

Abbildung 3: Testbericht von «AV-Comparatives.org»

Dieser Statistik nach zu urteilen scheinen die Antiviren-Programme, den Grossteil der Viren zu erkennen und zu eliminieren. Die Bedingungen des Tests wurden allerdings speziell gewählt. Unter der Vorgabe, dass ein reales Umfeld simuliert werden sollte, wurde angenommen, dass 40 – 50 % der zur Analyse eingefügten Webadressen direkt zu einer Schadsoftware führten, die restlichen 50 – 60 % hingegen zu einem so genannten *Exploit Pack*. Im Gegensatz zu Schadsoftware, die direkt auf den Computer gelangt, können Exploit Packs relativ gut durch Antiviren-Produkte geprüft und erkannt werden. Die hohe Erfolgsrate lässt sich dadurch erklären.

In einem ähnlichen Test mit statischen Bedingungen, der vom CRDF Threat Center[51], eine nicht kommerzielle, französische Webagentur, durchgeführt wurde und in dem die schädlichen Codes ausschliesslich auf ihren digitalen Signatur hin analysiert wurden, zeigte sich hingegen ein differenzierteres Bild. Zwar gab es Antiviren-Programme, die über 70 % der analysierten Codes als böswillig erkannten. Andere Produkte erkannten die Schadsoftware jedoch nur in 1 – 3 % der Fälle. Die durchschnittliche Erkennungsrate betrug laut dieser Studie 33 %.

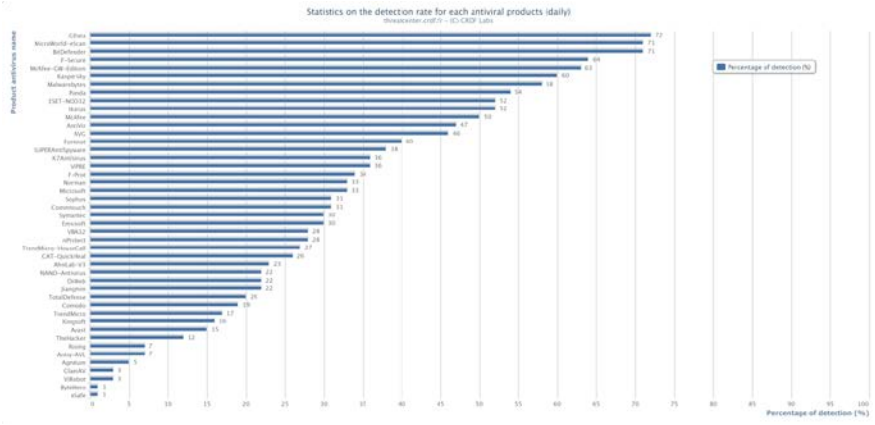


Abbildung 4: Testbericht vom «CRDF Threat Center»

51 https://threatcenter.crdf.fr/?Stats (Stand: 20. Februar 2014).

Wie sieht nun die Realität in der kriminellen Welt und insbesondere im Bereich der Wirtschaftskriminalität wirklich aus?

Um einer Detektion durch Antivirenprogramme zu entgehen, packen Kriminelle eine Malware oft mehrmals pro Tag neu. Bei diesem Packvorgang bleibt zwar der dahinterliegende Code identisch, er wird aber in einer Art und Weise zusammengestellt, dass er von aussen wie neu aussieht, um so nicht von Antiviren-Software erkannt zu werden. Kriminelle benutzen diesbezüglich sogar spezielle Plattformen, welche überprüfen, wie viele und welche Antivirenprogramme in der Lage sind, die neu gepackte Schadsoftware zu detektieren. Im Gegensatz zu den von Sicherheitsdienstleistern bereitgestellten Angeboten[52] wird bei den von den Kriminellen benutzten Plattformen allerdings penibel darauf geachtet, dass keinerlei Informationen über diese neuen Viren an die Antiviren-Hersteller gelangen.

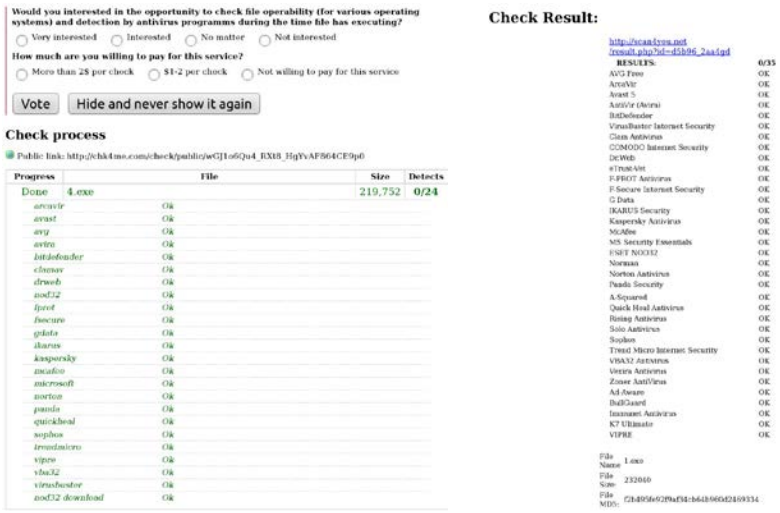


Abbildung 5: Beispiel eines von Kriminellen benutzten Antiviren-Checktools. Wenn bei einem Antivirenprodukt «o.k.» steht, bedeutet dies, dass der schädliche Code nicht als Virus erkannt wird. Falls ein Antivirenprodukt den Code als böswillig einstufen würde, würde der Kriminelle die Schadsoftware nochmals packen.

Bei so vielen Virenvarianten und Packprogrammen wird es für die Antiviren-Hersteller zunehmend schwieriger, nur mit Hilfe der Signatur die Schadsoftware zu identifizieren. Auch wenn die für Grundsicherheit erforderlichen Mindestvoraussetzungen (aktualisiertes System, *Firewall* und AV-Software) gültig bleiben, sind diese Massnahmen nicht mehr in der Lage, einen 100%igen Schutz zu gewährleisten.

Effizienz nur bei weitverbreiteter Schadsoftware

Die Effizienz der Anti-Viren-Produkte beschränkt sich insbesondere auf gängige weitverbreitete Schadsoftware. Bei gezielten Angriffen, die nur einen Bruchteil der Kunden betreffen, wird die Erkennung allerdings problematisch und praktisch unmöglich. Mikko Hypponen, Forschungsleiter bei F-Secure sagte mit Bezug auf Duqu, Flame, Gauss und Co.: «all of us had missed detecting this malware for two years, or more. That's a failure for our company, and for the antivirus industry in general»[53].

Auch wenn sich zielgerichtete Angriffe im Allgemeinen nicht gegen den gewöhnlichen Benutzer richten, hat man im Falle von Stuxnet gesehen, dass bei solchen Operationen auch Maschinen infiziert werden können, welche mit dem eigentlichen Ziel respektive dem

[52] Zum Beispiel Virustotal: http://www.virustotal.com (Stand: 20. Februar 2014).

[53] http://www.f-secure.com/weblog/archives/00002376.html (Stand: 20. Februar 2014).

potenziellen Opfer nichts zu tun haben. Aber auch im Bereich Wirtschaftskriminalität gibt es Tendenzen, kleinere Angriffe durch Ausnützung unbekannter Sicherheitslücken oder mit eigens für ein bestimmtes Ziel gepackter Schadsoftware durchzuführen, um somit unter dem Radar von Antivirenprodukten zu bleiben.

Neue Massnahmen sind gefragt

Man muss sich deshalb die Frage stellen, welche anderen Massnahmen erforderlich sind, um den Sicherheitsgrad zu erhöhen, damit auch kleinere und gezielte Angriffe erkannt werden können. Viele vor allem grössere Firmen setzten schon heute verschiedenste zusätzliche Systeme ein, um Anomalien und verdächtigen Internetverkehr zu detektieren und zu blockieren. Intelligente Detektionssysteme, welche den Firmennetzwerkverkehr analysieren und Abweichungen vom «Durchschnitt» erkennen, sind hier gefragt. Zu Firewall und Antiviren-Software gesellen sich Systeme zur Erkennung von Angriffen (*Intrusion Detection System*, IDS), weisse und *schwarze Listen* zur Filterung des Netzwerkverkehrs, das Überwachen (Monitoring) des Netzwerkverkehrs oder sogar das Monitoring des Verhaltens einzelner Computer dazu.

Ein weiterer Aspekt ist die Nachvollziehbarkeit. Sollte doch einmal eine (gezielte) Schadsoftware den Weg in das Firmennetzwerk gefunden haben, ist es sehr wichtig, nachvollziehen zu können, auf welchem Weg diese in das Firmennetzwerk gelangt ist und welche anderen Computer und Server ebenfalls involviert sind. Nur so hat man die Chance, die Schadsoftware komplett aus dem Netzwerk zu eliminieren. Wie die vergangenen Angriffe gezeigt haben, können zwischen dem Eindringen der Schadsoftware in das Netzwerk und dem Entdecken dieser Malware einige Monate oder sogar Jahre vergehen.[54] Eine Diskussion über die Aufbewahrungsdauer von *Logdaten* muss also ebenfalls geführt werden.

Eine weitere Erkenntnis aus den letzten Jahren ist, dass technische Massnahmen alleine nicht genügen. Am Schluss sind es immer die Mitarbeitenden, die die effizienteste Möglichkeit haben, einen Angriff zu erkennen und drauf richtig zu reagieren. Diesbezüglich ist eine regelmässige Schulung und Sensibilisierung der Mitarbeitenden von entscheidender Bedeutung. Ebenfalls wichtig ist die Schaffung einer Stelle, wo Mitarbeitende verdächtige Vorkommnisse melden können und auch ernst genommen werden.

Handlungsbedarf bei kleinen Unternehmen

Gerade bei kleinen Firmen besteht bezüglich zusätzlichen Cyberabwehrmassnahmen noch Handlungsbedarf. Diese sind vielfach nicht ausreichend gegen solche zielgerichteten Angriffe geschützt. Oftmals handelt es sich dabei um Nischenunternehmen, die ein beträchtliches Kapital in den Bereich Forschung und Entwicklung investiert haben und somit zu einem Ziel für mögliche gezielte Spionagetätigkeiten werden können. Gerade solche Firmen müssten Sicherheitssysteme einführen, die nicht ausschliesslich auf Antiviren-Software beruhen. Es geht vielfach vergessen, dass Kosten für die Implementierung von Sicherheitsmassnahmen dem Risiko von beträchtlichen Verlusten bei einem erfolgreichen Angriff gegenüberzustellen sind.

[54] Verizon: Data Breach Investigations Report 2012, Abbildung 40. Verfügbar unter http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf (Stand: 20. Februar 2014).

Schwierige Umsetzung im Privatbereich

Oben genannte Massnahmen können nicht auf Privatpersonen übertragen werden. Erweiterte und angemessene Sicherheitslösungen sind in einem solchen Fall zu kostenaufwändig. Zudem fehlen meist auch die Zeit und/oder das technische Know-How. Wie soll sich also der normale Computernutzer verhalten, welche Massnahmen kann er ergreifen?

Zukünftig wird es darum gehen, dass der private Nutzer vom eigenen Provider die Bereitstellung einer «sauberen» Internetverbindung fordern muss, auch wenn dies etwas kosten sollte. Dabei könnte der Provider die vorangehend genannten zusätzlichen Sicherheitsmassnahmen zentral für alle seine Kunden durchführen und ihnen so zusätzlichen Schutz bieten. Der Aspekt Sicherheit wird momentan von den Kunden kaum gefordert, umgekehrt werben Provider auch nicht mit dem Kriterium Sicherheit. Als Hauptkriterium beim Entscheid für einen Internetanschluss wird dann auch neben den Kosten meist nur die Geschwindigkeit herangezogen. Das wird sich in Zukunft ändern (müssen).

5.5 Angriffe auf Heimrouter

Heimrouter enthalten immer wieder unsichere Konfigurationen oder Sicherheitslücken. Während modernere Geräte von den Providern automatisiert mit Updates versehen werden können, ist das bei älteren Geräten nicht immer der Fall.

Unsichere Default-Konfigurationen (Standard- oder Werkeinstellungen)

Dienste, die bei Heimroutern für Distributed Denial of Service (DDoS) Angriffe missbraucht werden können, sind ein aktuell sehr ernst zu nehmendes Problem. Dabei stehen *DNS* und *NTP*, beide *UDP* basiert, im Zentrum. Ist ein solcher Dienst falsch konfiguriert und akzeptiert Anfragen aus dem gesamten Internet, können Angreifer diese für DDoS-Angriffe verwenden. Dabei wird oft die Tatsache ausgenutzt, dass mit einer relativ kleinen Anfrage eine grosse Antwort generiert wird (Amplifikation). Ein Teil dieser alten Geräte wurde mit unsicheren Default Konfigurationen ausgeliefert und lassen sich nicht durch Fernwartung mit einer aktuellen *Firmware* und/oder einer sicheren Konfiguration versehen. Viele Benutzer sind sich der Fehlkonfiguration ihres Gerätes und der damit verbundenen Gefahren gar nicht bewusst. Das Schadenspotenzial dieser Geräte ist jedoch riesig. Die Behebung dieser Fehlkonfigurationen ist aufwändig und zeitintensiv. MELANI ist in Kontakt mit den grossen Telecom-Providern, welche die Aktualisierung der verwundbaren Geräte durchführen müssen.

Sicherheitslücken auch in Routern

Es werden immer wieder Lücken in auf *ADSL*-Endgeräten verwendeten Firmwareversionen bekannt. Es gibt praktisch keinen Hersteller, der nicht schon Sicherheitslücken schliessen musste. Im Juni und Juli 2013 wurden verschiedene gravierende Sicherheitslücken in Geräten von Asus bekannt[55], ebenso eine Lücke im *UPnP* Dienst von D-Link Geräten.[56] Im Oktober 2013 wurde eine Lücke publiziert, bei der das einfache Ändern des «*User Agents*» im Browser reichte, um bei gewissen Netgear Geräten Zugang zum internen Webserver zu

[55] Bugtraq: http://seclists.org/bugtraq/2013/Jul/87 (Stand: 20. Februar 2014).

[56] Heise: http://www.heise.de/security/meldung/D-Link-Router-mit-schwerwiegender-UPnP-Luecke-1914510.html (Stand: 20. Februar 2014).

erhalten.[57] Auch bei weiteren Geräten von Netgear[58] und Draytek[59] gibt es Verwundbarkeiten, welche es einem Angreifer erlaubten, auf den Router zuzugreifen oder Schadcode auszuführen. Lücken dieser Art werden einerseits durch Würmer ausgenutzt, wie z.B. Linux.Darlioz[60], können aber auch von Kriminellen für das Umleiten von Online Banking Sessions genutzt werden.

MELANI empfiehlt den Zugang auf die Wartungsinterfaces der Router so stark als möglich einzuschränken. Viele Geräte unterstützen eine Restriktion auf eine *IP Adresse* aus dem internen Netz. Werden nicht vom Provider gewartete Geräte verwendet, muss der Benutzer selbstständig regelmässige Aktualisierungen einspielen. Zudem sollten nur Dienste aktiviert werden, die auch wirklich benötigt werden. Für die Behebung der OpenResolver Problematik, auch auf Heimgeräten, bietet Green eine ausführliche Anleitung an.[61]

5.6 Parlamentarische Geschäfte mit Bezug zu Themen im Bereich Informationssicherung

Ausgewählte parlamentarische Geschäfte im zweiten Halbjahr 2013 mit Bezug zu Themen im Bereich Informationssicherung.

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Fra	13.5284	Kontakt mit Edward Snowden zur Aufklärung der US-Spionage in der Schweiz	Glättli Balthasar	09.09.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135284
Fra	13.5283	Fehlende Reaktion des Bundesrates auf den Bruch der Privatsphäre von Schweizerinnen und Schweizern und Schweizer Firmen	Glättli Balthasar	09.09.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135283
Fra	13.5338	Flächendeckende Einführung von Vote électronique	Markwalder Christa	11.09.2013	NR	BK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135338
Fra	13.5334	Unkenntlichmachung von Luftaufnahmen sensibler Gebiete in öffentlich zugänglichen Dokumenten	van Singer Christian	11.09.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135334
Fra	13.5328	Vote électronique	Sommaruga Carlo	11.09.2013	NR	BK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135328
Fra	13.5319	Welche Massnahmen können zur Verhinderung von Datenschutzverletzungen durch die NSA getroffen werden	Schwaab Jean Christophe	11.09.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135319
Ip	13.3677	Schnüffeleien der NSA und anderen Nachrichtendienste auch in der Schweiz	Sozialdemokratische Fraktion / Tschümperlin Andy	11.09.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133677
Ip	13.3692	Telekommunikationsmarkt. Sind aktuelle Gesetzgebung und Regulierungsmassnahmen noch zeitgemäss?	Hurter Thomas	12.09.2013	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133692
Fra	13.5321	Wirtschaftsspionage der NSA auch in der Schweiz?	Leutenegger Oberholzer Susanne / SP Fraktion	16.09.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135321
Po	13.3707	Ganzheitliche und zukunftstaugliche Cyberraumstrategie	Fraktion BD / Guhl Bernhard	17.09.2013	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133707
Fra	13.5382	Exportkontrolle von Überwachungssoftware aus der Schweiz	Glättli Balthasar / Grüne Fraktion	18.09.2013	NR	WBF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135382
Fra	13.5380	Ungenügendes Instrumentarium zur Bekämpfung der Cyberkriminalität	Reinmann Maximilian	18.09.2013	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135380
Po	13.3736	Wi-Fi Strategie der Schweiz	Buttet Yannick	18.09.2013	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133736
Ip	13.3726	Identitätsmissbrauch. Eine Lücke im Strafrecht, die es zu füllen gilt?	Schwaab Jean Christophe	18.09.2013	NR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133726
Fra	13.1060	Missbrauch von Domain-Namen	Fehr Jacqueline	18.09.2013	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=2013

[57] Devttys0.com: http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/ (Stand: 20. Februar 2014).

[58] The Shadow File: http://shadow-file.blogspot.ch/2013/10/complete-persistent-compromise-of.html (Stand: 20. Februar 2014).

[59] CERT.org: http://www.kb.cert.org/vuls/id/101462 (Stand: 20. Februar 2014).

[60] Symantec: http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices (Stand: 20. Februar 2014).

[61] Green: http://www.green.ch/Portals/0/Support/pdf/Anleitung_OpenResolver_DE.pdf (Stand: 20. Februar 2014).

							1060
Pa.Iv.	13.445	In Schädigungsabsicht mittels digitaler Kommunikationsmittel begangenen Identitätsmissbrauch unter Strafe stellen	Golay Roger	18.09.2013	NR		http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20130445
Ip	13.3773	Zukunftstaugliches Fernmeldegesetz. Für eine übergreifende Cyberraumstrategie	Wasserfallen Christian	24.09.2013	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133773
Mo	13.3808	Nichts überstürzen bei der Ausdehnung von Vote électronique	Schwaab Jean Christophe	25.09.2013	NR	BK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133808
Ip	13.3799	IT-Sicherheit in der Bundesverwaltung. Welches Kosten-Nutzen-Verhältnis?	Cassis Ignazio	25.09.2013	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133799
Mo	13.3812	Kein unsicheres E-Voting. Nur Systeme mit Verifizierbarkeit und offenem Source Code zualssen	Glättli Balthasar	26.09.2013	NR	BK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133812
Mo	13.3841	Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit	Rechsteiner Paul	26.09.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133841
Mo	13.3930	Export von Überwachungs- und Spionagesoftware an Unrechtsstaaten verbieten	Glättli Balthasar	27.09.2013	NR	WBF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133930
Ip	13.3927	Schutz für den Datenbunker Schweiz	Reimann Lukas	27.09.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133927
Po	13.3989	Verletzung der Persönlichkeitsrechte im Zuge des Fortschritts der Informations- und Kommunikationstechnik	Recordon Luc	27.09.2013	SR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133989
Mo	13.4009	Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken	Sicherheitspolitische Kommission NR	05.11.2013	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134009
Ip	13.4023	Informatikpläne des Bundes	Fraktion CVP-EVP	27.11.2013	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134023
Po	13.4069	Spionage durch die NSA und andere ausländische Geheimdienste	Schwaab Jean Christophe	04.12.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134069
Ip	13.4077	Datenspionage und Internetsicherheit	Fraktion SVP	05.12.2013	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134077
Mo	13.4086	Nationales Forschungsprogramm Alltagstauglichkeit Datenschutz in der Informationsgesellschaft	Grüne Fraktion / Glättli Balthasar	05.12.2013	NR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134086
Mo	13.4091	Verbot der Nutzung von Einrichtungen zur politischen, militärischen oder wirtschaftlichen Spionage gegen die Schweiz oder andere Staaten	Grüne Fraktion / van Singer Christian	05.12.2013	NR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134091
Mo	13.4165	Nachrichtendienst-Affäre. No Spy-Abkommen mit den USA	Allemann Evi	12.12.2013	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134165
Po	13.4308	Sicherheit und Unabhängigkeit der Schweizer Informatik verbessern	Graf-Litscher Edith	13.12.2013	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134308

6 Glossar

3DES	Der Data Encryption Standard (DES) ist ein weit verbreiteter symmetrischer Verschlüsselungsalgorithmus.
Abuse-Stelle	Stelle eines Providers, wo Meldungen über verdächtige Vorkommnisse im Netzwerkbereich des Providers gemeldet werden können.
AdServer	AdServer werden zur Auslieferung und Erfolgsmessung von Internetwerbung eingesetzt. Sowohl der physische Server selbst, auf dem eine AdServer-Software läuft, als auch diese Software können als AdServer bezeichnet werden.
ADSL	Asymmetric Digital Subscriber Line. Eine Technologie, die einen schnellen und permanenten Internet-Zugang über die Telefonleitung ermöglicht.
Anonymisierungsdienst	Dienst, wie beispielsweise TOR, mit dessen Hilfe man eine fremde IP-Adresse verwenden kann, um die eigene Identität zu verbergen.
AntiVirus-Live-CD	CD von Antiviren-Software-Hersteller, welche noch vor dem Starten des Betriebssystems, den Computer auf Schadsoftware überprüft.
App	Der Begriff App (von der englischen Kurzform für Application) bezeichnet im Allgemeinen jede Form von Anwendungsprogrammen. Im Sprachgebrauch sind damit mittlerweile jedoch meist Anwendungen für moderne Smartphones und Tablet-Computer gemeint.
Applikationssoftware	Ein Computerprogramm, das eine bestimmte Aufgabe erfüllt. Textverarbeitungsprogramme und Internet Browser sind Beispiele für Applikationen.
APT	Diese Bedrohung führt zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder auf ein Land wirkt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen.
ARPANET	Das Arpanet (Advanced Research Projects Agency Network) wurde ursprünglich im Auftrag der US-Luftwaffe ab 1962 von einer kleinen Forschergruppe unter der Leitung des Massachusetts Institute of Technology und des US-Verteidigungsministeriums entwickelt. Es ist der

	Vorläufer des heutigen Internets.
Attachments/ Anhang	Ein Attachment ist eine Datei , die als Anlage an den Text einer E-Mail verschickt wird.
Backdoor	Backdoor (deutsch: Hintertür) bezeichnet einen Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
Backup	Backup (deutsch Datensicherung) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können.
Black- / White-List	Black-List (schwarze Liste): Liste von Instanzen wie zum Beispiel Webseiten, die im Vergleich zur Allgemeinheit benachteiligt werden sollen. Die Benachteiligung kann sich beispielsweise in einer Sperre der entsprechenden Webseite äussern. White-List (weisse Liste): Liste von Instanzen, die nach der Meinung des Verfassers der White-List grundsätzlich vertrauenswürdig sind.
Botnetz	Eine Ansammlung von Computern, die mit Malicious Bots infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen hundert bis millionen kompromittierter Rechner bestehen.
Command and Control-Server	Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet.
Content Management Systemen (CMS)	Ein Content-Management-System (kurz: CMS, übersetzt: Inhaltsverwaltungssystem) ist ein System, das die gemeinschaftliche Erstellung und Bearbeitung von Inhalt, bestehend aus Text- und Multimedia-Dokumenten, ermöglicht und organisiert, meist für das World Wide Web. Ein Autor kann ein solches System auch ohne Programmier- oder HTML-Kenntnisse bedienen. Der darzustellende Informationsgehalt wird in diesem Zusammenhang als Content (Inhalt) bezeichnet.
Cross Site Scripting	Cross-Site-Scripting (XSS; deutsch Website-übergreifendes Scripting) bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden.

Distributed Denial Of Service (DDoS)	Distributed-Denial-of-Service Attacke. Eine DoS Attacke, bei der das Opfer von vielen verschiedenen Systemen aus gleichzeitig angegriffen wird.
DNS-Dienste	Domain Name System. Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
Domäne	Der Domain Name (z. B. www.example.com) kann durch das DNS (Domain Name System) in eine IP-Adresse aufgelöst werden, die dann verwendet werden kann, um Netzwerkverbindungen zu diesem Rechner aufzubauen.
Drive-By Downloads	Infektion eines Computers mit Malware allein durch den Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
Exploit Pack	Ein Baukasten mit dessen Hilfe sich Schadsoftware herstellen lässt, welche Schwachstellen in Computersystemen ausnutzt.
Fernzugang (Remote Access)	Die Fernwartungssoftware (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar.
Firmware	Befehlsdaten zur Steuerung eines Gerätes (z.B. Scanner, Grafikkarten, usw.), die in einem Chip gespeichert sind. Diese Daten können in der Regel über Upgrades geändert werden.
Hash	Algorithmus welcher aus einem beliebigen Text eine Zahlenfolge generiert. Hashfunktionen werden in drei Bereichen verwendet: - In der Kryptografie. - Bei Datenbanksystemen. Diese verwenden Hashfunktionen, um in grossen Datenbankbeständen effizient zu suchen. - Bei Prüfsummen. Jeder Datei kann ein Hashwert zugeordnet werden. Ein veränderter Hashwert deutet auf eine Manipulation hin.
Heimrouter	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die meh-

	rere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.
Hosting	Hosting ist die Unterbringung von Internetprojekten, die sich in der Regel auch öffentlich durch das Internet abrufen lassen.
HTML	HyperText Markup Language. In HTML werden die Webseiten erstellt. Damit lassen sich die Eigenschaften der Webseiten (z.B. der Seitenaufbau, das Layout, die Links auf andere Seiten, usw.) vorgeben. Da HTML aus ASCII-Zeichen besteht, kann eine HTML-Seite mit einem gewöhnlichen Textverarbeitungsprogramm bearbeitet werden.
IFrame	Ein IFrame (auch Inlineframe) ist ein HTML-Element, das der Strukturierung von Webseiten dient. Es wird benutzt, um externe Webinhalte in der eigenen Homepage einzubinden.
Internet Explorer Cache	Cache bezeichnet in der EDV einen schnellen Puffer-Speicher, der (erneute) Zugriffe auf ein langsames Hintergrundmedium oder aufwändige Neuberechnungen zu vermeiden hilft.
IP Adresse	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
Java	Java ist eine objektorientierte Programmiersprache und eine eingetragene Marke des Unternehmens Sun Microsystems (2010 von Oracle aufgekauft).
Laufwerksbuchstaben	Microsoft-Betriebssysteme repräsentieren die Laufwerke (genauer: deren Partitionen, die so dem Benutzer wie eigene Laufwerke erscheinen) durch Großbuchstaben.
Life Cycle Management	Der Produktlebenszyklus ist ein Konzept der Betriebswirtschaftslehre und beschreibt den Prozess zwischen der Markteinführung bzw. Fertigstellung eines marktfähigen Gutes und seiner Herausnahme aus dem Markt.
Logdaten	Eine Logdatei enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem.
Random-Access Memory (RAM)	Random-Access Memory (RAM)ist ein Informations-Speicher, der besonders bei Computern als Arbeitsspeicher Verwendung findet, meist in Form von Speichermodulen.

mTAN	Die Variante Mobile TAN (mTAN) oder smsTAN besteht aus der Einbindung des Übertragungskanals SMS. Die Transaktionsnummer (TAN) wird in Form einer SMS gesendet.
Netzlaufwerke	Sofern auf eine Dateifreigabe im Netzwerk eine permanente Verbindung eingerichtet wird, entsteht ein Netzlaufwerk, das als virtuelles Laufwerk die Ordner und Dateien eines Servers auf dem Client wie gewohnt anzeigt.
NTP-Protokoll	Das Network Time Protocol (NTP) ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze.
Open Source	Open Source ist eine Palette von Lizenzen für Software, deren Quelltext öffentlich zugänglich ist und durch die Lizenz Weiterentwicklungen fördert.
Over-the-air-Technologie	Die Luftschnittstelle bezeichnet die Übertragung von Daten mittels elektromagnetischer Wellen durch das Medium Luft (over the air, Abkürzung OTA).
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
PHP Code	PHP ist eine Skriptsprache, die hauptsächlich zur Erstellung von dynamischen Webseiten oder Webanwendungen verwendet wird.
PIN	Eine Persönliche Identifikationsnummer (PIN) oder Geheimzahl ist eine Zahl, mit der man sich gegenüber einer Maschine authentisieren kann.
Point of Sales (POS)	Ein POS-Terminal (in der Schweiz EFT/POS-Terminal) ist ein Online-Terminal zum bargeldlosen Bezahlen an einem Verkaufsort (Point of Sale).
Proprietär	Das Adjektiv proprietär bedeutet in Eigentum befindlich. Es wird in Bezug auf Soft- und Hardware verwendet, um diese zu freier Software und freier Hardware abzugrenzen.

Quellcode	Der Begriff Quelltext, auch Quellcode (engl. source code) genannt, bezeichnet in der Informatik der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes.
Ransomware	Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt oder gelöscht und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.
Roaming	Der Begriff Roaming oder Durchleitung stammt ursprünglich aus dem Bereich des GSM-Funknetzes. Herkömmliches GSM-Roaming ist die Fähigkeit eines Mobilfunknetz-Teilnehmers, in einem anderen, fremden Netzwerk als seinem Heimnetzwerk selbsttätig Anrufe zu empfangen oder zu tätigen, Daten zu schicken und zu empfangen oder Zugriff auf andere Mobilfunknetzdienste zu haben.
Rootkit	Auswahl an Programmen und Technologien, welche den unbemerkten Zugang und die unbemerkte Kontrolle eines Computers ermöglichen.
Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). Siehe auch Malware.
Schlüssel	Als Schlüssel wird in der Kryptologie allgemein eine Information bezeichnet, die einen kryptographischen Algorithmus parametrisiert.
Schwachstellen	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Scriptcode / Javascript	Eine objektbasierte Scriptingsprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.

SIM Karte	Die SIM-Karte (englisch: Subscriber Identity Module) ist eine Chipkarte, die in ein Mobiltelefon eingesteckt wird und zur Identifikation des Nutzers im Netz dient.
SMS	Short Message Service Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Social Engineering	Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen.
Sourcecode	Unter dem Begriff Quellcode (englisch source code) wird in der Informatik der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes verstanden.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
Spear phishing	Gezielte Phishing Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren.
SQL Injection	SQL-Injection (SQL-Einschleusung) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Überprüfung von zu übermittelnden Variablen entsteht. Der Angreifer versucht dabei eigene Datenbankbefehle einzuschleusen, um Daten in seinem Sinne zu verändern oder Kontrolle über den Server zu erhalten.
SSH-Dämon	Secure Shell Protokoll, mit dem dank Datenverschlüsselung u.a. das sichere Anmelden (Login) an einem über ein Netzwerk (z.B. Internet) zugänglichen Computersystem möglich ist. Ein Daemon ist ein Programm, das im Hintergrund abläuft.
Stream	Mit Datenströmen (englisch data streams) bezeichnet man in der Informatik kontinuierliche Abfolgen von Datensätzen, deren Ende nicht im Voraus abzusehen ist.
UDP	User Datagram Protocol (UDP) ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie ge-

	hört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.
UPnP	Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Audio-Geräte, Router, Drucker, Haussteuerungen) über ein IP-basiertes Netzwerk, mit oder ohne zentrale Kontrolle durch ein Residential Gateway.
User Agents	Ein User Agent ist ein Client-Programm, mit dem ein Netzwerkdienst genutzt werden kann.
Watering-Hole Angriffe	Gezielte Infektion durch Schadsoftware über Webseiten, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden.
Zwei-Faktor-Authentisierung	Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z.B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z.B. Zertifikat, Token, Streichliste, usw.) 3. Etwas, das man ist (z.B. Fingerabdruck, Retina-Scan, Stimmerkennung, usw.)